

35.G2550



PATENT APPLICATION

#6
KUS
17740

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)	
	:	Examiner: Unknown
SATORU WAKAO, ET AL.)	
	:	Group Art Unit: Unknown
Appln. No.: 09/521,424)	
	:	
Filed: March 8, 2000)	
	:	
For: IMAGE PROCESSING)	May 31, 2000
APPARATUS AND IMAGE	:	
PROCESSING METHOD)	

Assistant Commissioner For Patents
Washington, D.C. 20231

CLAIM TO PRIORITY

Sir:

Applicants hereby claim priority under the
International Convention and all rights to which they are
entitled under 35 U.S.C. § 119 based upon the following Japanese
Priority Applications:

11-063174, filed March 10, 1999; and
2000-057077, filed March 2, 2000.

A certified copy of the priority document is enclosed.

Applicants' undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should be directed to our below-listed address.

Respectfully submitted,


Attorney for Applicants

Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

BLK/fdb

SATORU WAKAO, ET AL
Appln. No. 09/521,4

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年 3月10日

出 願 番 号
Application Number:

平成11年特許願第063174号

出 願 人
Applicant(s):

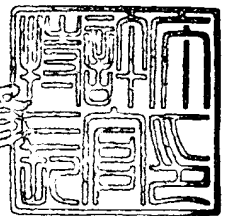
キヤノン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 3月31日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3022382

【書類名】 特許願

【整理番号】 3858035

【提出日】 平成11年 3月10日

【あて先】 特許庁長官 伊佐山 建志 殿

【国際特許分類】 G06F 15/00
H04N 7/00

【発明の名称】 画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体

【請求項の数】 42

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社
内

【氏名】 若尾 聡

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社
内

【氏名】 岩村 恵市

【特許出願人】

【識別番号】 000001007

【住所又は居所】 東京都大田区下丸子3丁目30番2号

【氏名又は名称】 キャノン株式会社

【代表者】 御手洗 富士夫

【電話番号】 03-3758-2111

【代理人】

【識別番号】 100069877

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社
内

【弁理士】

【氏名又は名称】 丸島 儀一

【電話番号】 03-3758-2111

【手数料の表示】

【予納台帳番号】 011224

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9703271

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体

【特許請求の範囲】

【請求項 1】 デジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、

前記演算手段の出力を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする画像処理装置。

【請求項 2】 請求項 1 において、前記演算手段は、前記デジタル画像と前記秘密情報とを用いて逆演算可能な演算を行うことを特徴とする画像処理装置。

【請求項 3】 請求項 1 若しくは 2 において、前記生成手段は、前記演算手段の演算結果に対して一方向関数を用いた演算を行うことを特徴とする画像処理装置。

【請求項 4】 請求項 3 において、前記一方向性関数は、ハッシュ関数であることを特徴とする画像処理装置。

【請求項 5】 請求項 3 において、前記一方向性関数は、共通鍵暗号を実現する関数であることを特徴とする画像処理装置。

【請求項 6】 請求項 1 ～ 5 の何れかにおいて、前記生成手段は、前記デジタル画像毎に、該デジタル画像に対応する署名データを生成することを特徴とする画像処理装置。

【請求項 7】 請求項 1 ～ 6 の何れかにおいて、前記生成手段は、前記演算手段の出力を用いて、前記デジタル画像に対する不正な処理を検出するため署名データを生成するプログラムに従って前記デジタル画像に対応する署名データを生成することを特徴とする画像処理装置。

【請求項 8】 請求項 1 ～ 7 の何れかにおいて、前記秘密情報は、前記画像処理装置を識別するための情報であることを特徴とする画像処理装置。

【請求項 9】 請求項 1～7 の何れかにおいて、前記秘密情報は、前記画像処理装置と接続可能な外部装置を識別するための情報であることを特徴とする画像処理装置。

【請求項 10】 請求項 1～7 の何れかにおいて、前記秘密情報は、前記画像処理装置と接続可能な外部装置を使用するユーザを識別するための情報であることを特徴とする画像処理装置。

【請求項 11】 請求項 1～10 の何れかにおいて、前記署名データの生成に必要な演算の少なくとも一部を、前記画像処理装置に接続された外部装置に演算させることを特徴とする画像処理装置。

【請求項 12】 請求項 1～11 の何れかにおいて、前記デジタル画像は、圧縮符号化されていることを特徴とする画像処理装置。

【請求項 13】 請求項 1～12 の何れかにおいて、前記画像処理装置は更に、前記デジタル画像を生成する撮像部を具備することを特徴とする画像処理装置。

【請求項 14】 請求項 1～13 の何れかにおいて、前記画像処理装置は更に、前記デジタル画像と前記署名データとを出力可能なデジタルインタフェースを具備することを特徴とする画像処理装置。

【請求項 15】 請求項 1～14 の何れかにおいて、前記画像処理装置は更に、前記前記デジタル画像データと前記署名データとを所定の記録媒体に記録する記録手段を具備することを特徴とする画像処理装置。

【請求項 16】 デジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、

前記演算手段の出力と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する検出手段とを具備することを特徴とする画像処理装置。

【請求項 17】 請求項 16 において、前記演算手段は、前記デジタル画像と前記秘密情報とを用いて逆演算可能な第 1 の演算を行うことを特徴とする画像処理装置。

【請求項 18】 請求項 17 において、前記演算手段は、前記第 1 の演算の結果に対して一方向関数を用いた第 2 の演算を行うことを特徴とする画像処理装置。

【請求項 19】 請求項 16～18 の何れかにおいて、前記画像処理装置は、前記デジタル画像毎に、該デジタル画像に対する不正な処理の有無を検出することを特徴とする画像処理装置。

【請求項 20】 請求項 16～19 の何れかにおいて、前記検出手段は、前記演算手段の出力と前記署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出するプログラムに従って前記デジタル画像に対する不正な処理の有無を検出することを特徴とする画像処理装置。

【請求項 21】 請求項 16～20 の何れかにおいて、前記画像処理装置は更に、前記検出手段の検出結果を表示する表示手段を具備することを特徴とする画像処理装置。

【請求項 22】 デジタル画像と秘密情報とを用いて所定の演算を行う第 1 の演算手段と、

前記第 1 の演算手段の出力を用いて、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備する第 1 の画像処理装置と、

前記デジタル画像と前記秘密情報とを用いて所定の演算を行う第 2 の演算手段と、

前記第 2 の演算手段の出力と前記署名データとを比較して該デジタル画像に対する不正な処理の有無を検出する検出手段とを具備する第 2 の画像処理装置とにより構成することを特徴とする画像処理システム。

【請求項 23】 デジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする画像処理方法。

【請求項 24】 デジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出するこ

とを特徴とする画像処理方法。

【請求項 25】 デジタル画像と秘密情報とを用いて所定の演算を行う手順と、

該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項 26】 デジタル画像と秘密情報とを用いて所定の演算を行う手順と、

該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項 27】 デジタル画像を生成する撮像手段と、

前記デジタル画像と秘密情報とを用いて所定の演算を行い、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする撮像装置。

【請求項 28】 請求項 27 において、前記生成手段は、前記デジタル画像と前記秘密情報とを用いて逆演算可能な第 1 の演算を行うことを特徴とする画像処理装置。

【請求項 29】 請求項 28 において、前記生成手段は、前記第 1 の演算の結果に対して一方向関数を用いた第 2 の演算を行うことを特徴とする画像処理装置。

【請求項 30】 請求項 29 において、前記一方向性関数は、ハッシュ関数であることを特徴とする撮像装置。

【請求項 31】 請求項 29 において、前記一方向性関数は、共通鍵暗号を実現する関数であることを特徴とする撮像装置。

【請求項 32】 請求項 29 において、前記生成手段は、前記撮像手段が前記デジタル画像を生成する毎に、該デジタル画像に対応する署名データを生成することを特徴とする撮像装置。

【請求項 33】 請求項 27～32 の何れかにおいて、前記生成手段は、前記撮像手段により生成されたデジタル画像と秘密情報とを用いて所定の演算を行い、該デジタル画像に対する不正な処理を検出するための署名データを生成するプログラムに従って前記デジタル画像に対応する署名データを生成することを特徴とする撮像装置。

【請求項 34】 請求項 27～33 の何れかにおいて、前記秘密情報は、前記撮像装置を識別するための情報であることを特徴とする撮像装置。

【請求項 35】 請求項 27～33 の何れかにおいて、前記秘密情報は、前記撮像装置と接続可能な外部装置を識別するための情報であることを特徴とする撮像装置。

【請求項 36】 請求項 27～33 の何れかにおいて、前記秘密情報は、前記撮像装置と接続可能な外部装置を使用するユーザを識別するための情報であることを特徴とする撮像装置。

【請求項 37】 請求項 27～36 の何れかにおいて、前記署名データの生成に必要な演算の少なくとも一部を、前記撮像装置に接続された外部装置に演算させることを特徴とする撮像装置。

【請求項 38】 請求項 27～37 の何れかにおいて、前記デジタル画像は、圧縮符号化されていることを特徴とする撮像装置。

【請求項 39】 請求項 27～38 の何れかにおいて、前記撮像装置は更に、前記デジタル画像と前記署名データとを出力可能なデジタルインタフェースを具備することを特徴とする撮像装置。

【請求項 40】 請求項 27～39 の何れかにおいて、前記撮像装置は更に、前記前記デジタル画像と前記署名データとを所定の記録媒体に記録する記録手段を具備することを特徴とする撮像装置。

【請求項 41】 デジタル画像を撮像し、
該デジタル画像と秘密情報とを用いて所定の演算を行い、
該デジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする撮像方法。

【請求項 4 2】 撮像部により撮像されたデジタル画像と、秘密情報とを用いて所定の演算を行う手順と、

該デジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体に係り、特にデジタル画像情報の著作権を保護するための技術、デジタル画像情報に対する不正な処理を検出するための技術に関するものである。

【0002】

【従来の技術】

近年、撮影した画像を従来の銀塩写真や 8 mm フィルムに記録するのではなく、デジタルデータとして記録媒体に記録する画像入力装置（例えば、デジタルカメラ）が実用化されている。

【0003】

【発明が解決しようとする課題】

ところが、通常デジタルデータは、アナログデータと異なり加工が容易で、改竄、偽造、合成等を簡単に行うことができる。このため、デジタルデータは、銀塩写真等と比較して信憑性が低く、証拠能力に乏しいという問題があった。

【0004】

このような問題を解決するために、デジタルデータに対する改竄、偽造、合成等を検出するための技術が提案されている。例えば、この技術の一例として、ハッシュ関数と公開鍵暗号方式とを組み合わせたシステムが提案されている。

【0005】

以下、図 28 を用いてそのシステムを説明する。ここで、公開鍵暗号方式は、暗号鍵と復号鍵とが異なり、暗号鍵を公開し、復号鍵を秘密に保持する方式であ

る。

【0 0 0 6】

まず、送信側（出力側）の構成と動作について説明する。

【0 0 0 7】

①デジタルデータMをハッシュ関数Hを用いて圧縮し、一定長の出力hを演算する。

【0 0 0 8】

②暗号鍵K_eを用いて上述のhを暗号化し、出力sを求める。この出力sをデジタル署名データと呼ぶ。

【0 0 0 9】

③出力回路は、デジタル署名データsとデジタルデータMとを一組として出力する。

【0 0 1 0】

次に、受信側（検出側）構成と動作について説明する。

【0 0 1 1】

④デジタルデータMとそれに対応するデジタル署名データsとを入力する。

【0 0 1 2】

⑤デジタル署名データsを暗号鍵K_eに対応する復号鍵K_dで復号し、出力h''を生成する。

【0 0 1 3】

⑥デジタルデータMを送信側と同じハッシュ関数Hを用いて演算し、出力h'を求める。

【0 0 1 4】

⑦比較回路は、⑤で求めた出力h''と⑥で求めた出力h'とを比較し、一致すれば入力されたデジタルデータMを不正な処理のされていない正当なデータであると判断し、不一致であれば不正な処理のされたデータと見なす。

【0 0 1 5】

つまり、ハッシュ関数Hと暗号鍵K_eとを用いてデジタル署名データsを生

成することによって、デジタルデータMに対する改竄、偽造、合成等を検出することができる。

【0016】

しかしながら、上述のシステムには次のような問題があった。

【0017】

例えば、公開鍵暗号方式の暗号化回路及び復号化回路の構成は複雑で小型化が難しく、それらの回路の演算量は膨大で、処理時間が長くなる欠点があった。特に、公開鍵暗号方式では、べき乗演算と剰余演算とが必要であり、共通鍵暗号方式（暗号鍵と復号鍵とが同一となる暗号方式）に比べて演算が複雑且つ膨大となるため、処理の高速化が大変難しかった。そのため、高速な処理の実現は難しく、小型で安価なシステムをユーザに提供しにくい問題があった。

【0018】

又、処理時間を早くするためには、より高性能のCPU（中央演算処理装置）とより大容量のメモリとを用いて、ハードウェアの性能を向上させる必要がある。しかしながら、それではシステム全体の大規模化やコストアップを招くだけで安価で小型で高速なシステムをユーザに提供しにくい問題があった。

【0019】

以上の背景から本出願の発明の目的は、デジタルデータの著作権を保護すると共に、そのデジタルデータに対する不正な処理を簡単な構成で、高速に検出することのできる画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体を提供することである。

【0020】

又、本出願の発明の目的は、デジタルデータの著作権を保護すると共に、そのデジタルデータが不正に処理されていないことを検証するためのデータを簡単な構成で、高速に生成することのできる画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体を提供することである。

【0021】

又、本出願の発明の目的は、デジタルデータが不正に処理されていないこと

を検証するためのデータを用いて、そのデジタルデータに対する不正な処理を簡単な構成で、高速に検出することのできる画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体を提供することである。

【0022】

【課題を解決するための手段】

上述のような目的を達成するために、本発明の画像処理装置は、デジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、前記演算手段の出力を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする。

【0023】

又、本発明の画像処理装置は、デジタル画像と秘密情報とを用いて所定の演算を行う演算手段と、前記演算手段の出力と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する検出手段とを具備することを特徴とする。

【0024】

又、本発明の画像処理システムは、デジタル画像と秘密情報とを用いて所定の演算を行う第1の演算手段と、前記第1の演算手段の出力を用いて、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備する第1の画像処理装置と、前記デジタル画像と前記秘密情報とを用いて所定の演算を行う第2の演算手段と、前記第2の演算手段の出力と前記署名データとを比較して該デジタル画像に対する不正な処理の有無を検出する検出手段とを具備する第2の画像処理装置とにより構成することを特徴とする。

【0025】

又、本発明の画像処理方法は、デジタル画像と秘密情報とを用いて所定の演算を行い、該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする。

【0026】

又、本発明の画像処理方法は、デジタル画像と秘密情報とを用いて所定の演

算を行い、該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出することを特徴とする。

【0027】

又、本発明のコンピュータ読み取り可能な記憶媒体は、デジタル画像と秘密情報とを用いて所定の演算を行う手順と、該演算結果を用いて、前記デジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【0028】

又、本発明のコンピュータ読み取り可能な記憶媒体は、デジタル画像と秘密情報とを用いて所定の演算を行う手順と、該演算結果と、前記デジタル画像に対する不正な処理を検出するための署名データとを比較して前記デジタル画像に対する不正な処理の有無を検出する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【0029】

又、本発明の撮像装置は、デジタル画像を生成する撮像手段と、前記デジタル画像と秘密情報とを用いて所定の演算を行い、該デジタル画像に対する不正な処理を検出するための署名データを生成する生成手段とを具備することを特徴とする。

【0030】

又、本発明の撮像方法は、デジタル画像を撮像し、該デジタル画像と秘密情報とを用いて所定の演算を行い、該デジタル画像に対する不正な処理を検出するための署名データを生成することを特徴とする。

【0031】

又、本発明のコンピュータ読み取り可能な記憶媒体は、撮像部により撮像されたデジタル画像と、秘密情報とを用いて所定の演算を行う手順と、該デジタル画像に対する不正な処理を検出するための署名データを生成する手順とを実行させるためのプログラムを記憶したことを特徴とする。

【0032】

【発明の実施の形態】

以下、本発明の画像処理装置、方法及びシステム、並びに撮像装置、撮像方法、コンピュータ読み取り可能な記憶媒体について図面を用いて詳細に説明する。

【0033】

(基本構成)

まず、図1を用いて、各実施例に共通するデジタル画像検証システムの基本構成と処理手順とについて説明する。

【0034】

図1において、画像入力装置10は、デジタル画像データP11と秘密情報S12とに基づいてデジタル署名データh13を生成する。具体的に、画像入力装置10は、秘密情報S12を用いてデジタル画像データP11にある操作（例えば、付加、多重、或いは合成）を加え、その結果を一方向性関数（例えば、ハッシュ関数等の逆関数の生成が困難或いは不可能な関数）で演算し、その演算結果からデジタル署名データh13を生成する。このデジタル署名データh13は、対応するデジタル画像データP11と共に一時的に記録され、必要に応じて外部出力される。

【0035】

又、図1において、画像検証装置20は、デジタル画像データP'21と共にデジタル署名データh'23を外部入力する。画像検証装置20は、デジタル画像データP'21と秘密情報S22（上述の秘密情報S12と同一の情報である）とを用いて画像入力装置10と同様の処理を行い、デジタル署名データh''24を生成する。

【0036】

このデジタル署名データh''24は、デジタル画像データP'21と共に外部入力されたデジタル署名データh'23と比較される。両者が一致した場合、画像検証装置20は、デジタル画像データP'21を不正な処理のされていない正当なデータであると判断する。又、デジタル画像データP'21が外部入力される前に改竄されていた場合、両者は不一致となるため、デジタル画

像データ P' 21 を不正に処理されたデータであると判断する。このような手順により、画像検証装置 20 は、外部入力されたデジタル画像データ P' 21 に対して不正な処理（例えば、改竄、偽造、合成等）が施されているか否かを検出することができる。

【0037】

尚、図 1 において、画像入力装置 10 と画像検証装置 20 とは、同一の秘密情報を共有する。この秘密情報は、読み出し専用の記録媒体等に記録され、外部に漏れることがないように管理されている。

【0038】

以上のように、本実施例のデジタル画像検証システムでは、秘密情報 S 12 を用いてデジタル画像データ P 11 にある操作を加え、その結果を一方向性関数演算し、その演算結果からデジタル署名データ h 13 を生成している。

【0039】

このような処理によって得られたデジタル署名データ h 13 は、デジタル画像データ P 11 と秘密情報 S 12 とに対して固有の情報となるため、不正なユーザは、秘密情報 S 12 を知らなければ、デジタル画像データ P 11 を改竄したとしても、そのデジタル画像データ P 11 に対応するデジタル署名データ h 13 を不正に作り出すことはできない。又、不正なユーザは、一方向性関数の性質により、得られたデジタル署名データ h 13 から元のデータ（即ち、秘密情報 S 12 を用いてある操作を加えたデジタル画像データ P 11）を知ることができない。

【0040】

これにより、本実施例では、複雑な暗号化技術を用いることなく、簡単で安価な回路構成と少ない演算量で高速にデジタル署名データを生成することができ、デジタル画像データの著作権を保護し、該デジタル画像データに対する不正な処理（改竄、偽造、合成等）を確実に検出することができる。

【0041】

次に、図 1 に示す画像入力装置 10 及び画像検証装置 20 の基本構成について詳細に説明する。

【0042】

(1) 画像入力装置の構成

図2は、画像入力装置10の構成の一例を示す図である。ここで、画像入力装置10は、デジタルカメラ、カメラ一体型デジタルレコーダ、スキャナ等の撮像機能を有する電子機器である。

【0043】

図2において、撮像部201は、CCDやレンズ等からなり、被写体の光学像を電気信号に変換し、その電気信号を更に所定フォーマットのデジタル画像データに変換する。作業用メモリ202は、デジタル画像データ等を一時的に保管し、デジタル画像データに対する高能率符号化処理、後述のデジタル署名データの生成等に使用される。

【0044】

記録再生部203は、取り外し可能な記録媒体（例えば、メモリカード等）を有し、撮像部201により生成され、高能率符号化されたデジタル画像データとそれに対応するデジタル署名データとを一組として記録する。駆動部204は、撮像部201や記録再生部203の機械的動作を制御する。

【0045】

外部インタフェース部205は、1つ以上の外部装置と接続可能なデジタルインタフェースであり、例えば、デジタル署名データの付加されたデジタル画像データを所定の外部装置に送信することができる。

【0046】

制御／演算部206は、ROM207に格納されている各種のプログラムに従って画像入力装置全体の動作を制御する制御回路210、デジタル画像データを高能率符号化（例えば、DCT変換やウェーブレット変換されたデジタル画像データを量子化し、可変長符号化する）する画像処理回路211、後述のデジタル署名データの生成に必要なハッシュ関数演算や各種の演算処理を行う演算回路212、デジタル署名データの生成に必要な秘密情報（例えば、画像入力装置10を識別するためのID情報等）を格納するメモリ213、演算回路212に必要な乱数を生成する乱数発生回路214を含む。

【0047】

ROM 2 0 7 は読み出し専用メモリであり、画像入力装置 1 0 全体の動作を制御するプログラム、画像処理を制御するプログラム、デジタル署名データを生成処理を制御するプログラム等を格納している。操作部 2 0 8 は、ユーザからの各種の指示を受け付け、その指示に対応する制御信号を制御／演算部 2 0 6 に供給する。

【0048】

(2) 画像検証装置の構成

図 3 は、画像検証装置 2 0 の構成の一例を示す図である。ここで、画像検証装置 2 0 は、パーソナルコンピュータ、ワークステーション等の情報処理装置やそれに接続可能な拡張ボードである。

【0049】

図 3 において、外部インタフェース部 3 0 1 は、外部のネットワークからデジタル署名データの付加されたデジタル画像データ（ここで、デジタル画像データは、高能率符号化されている）を入力するデジタルインタフェースである。又、外部インタフェース部 3 0 1 は、取り外し可能な記録媒体（例えば、メモリカード等）とも接続可能である。そして、その記録媒体に記録されたデジタル画像データをデジタル署名データと共に入力する。

【0050】

作業用メモリ 3 0 2 は、デジタル画像データ等を一時的に保管し、デジタル画像データに対する伸長復号処理、後述のデジタル署名データの生成等に使われる。

【0051】

制御／演算部 3 0 3 は、ROM 3 0 5 に格納されている各種のプログラムに従って画像検証装置全体の動作を制御する制御回路 3 1 0、デジタル画像データを伸長復号（例えば、可変長復号し、逆量子化した後、逆 D C T 変換や逆ウェーブレット変換する）する画像処理回路 3 1 1、後述のデジタル署名データの生成に必要なハッシュ関数演算やデジタル画像データを検証するための演算処理を行う演算回路 3 1 2、デジタル署名データの生成に必要な秘密情報を格納す

るメモリ 3 1 3、演算回路 3 1 2に必要な乱数を生成する乱数発生回路 3 1 4を含む。

【 0 0 5 2 】

表示部 3 0 4 は、デジタル画像データを視覚的に表示する。又、表示部 3 0 4 は、そのデジタル画像データの検証結果をユーザに視覚的に表示できる。尚、表示部 3 0 4 は、画像検証装置 2 0 と取り外し可能である。

【 0 0 5 3 】

ROM 3 0 5 は、読み出し専用メモリであり、画像検証装置 2 0 全体の動作を制御するプログラム、画像処理を制御するプログラム、デジタル画像データの検証処理を制御するプログラムを格納している。操作部 3 0 6 は、ユーザからの各種の指示を受け付け、その指示に対応する制御信号を制御／演算部 3 0 3 に供給する。

【 0 0 5 4 】

以下、第 1 ～第 6 の実施例では、図 2 の画像入力装置 1 0 が、デジタル画像データと秘密情報とに基づいてデジタル署名データを生成する手順について詳細に説明する。

【 0 0 5 5 】

又、第 7 ～第 1 2 の実施例では、図 3 の画像検証装置 2 0 が、画像入力装置 1 0 にて生成されたデジタル署名データに基づいてデジタル画像データの正当性を検証する手順について詳細に説明する。

【 0 0 5 6 】

(第 1 の実施例)

第 1 の実施例では、画像入力装置 1 0 が、機器固有の秘密情報とハッシュ関数とを用いてデジタル署名データを生成する処理について説明する。具体的に第 1 の実施例では、デジタル画像データと機器固有の秘密情報とを用いて予め定められた規則の演算を行い、その演算結果をハッシュ関数を用いて演算し、その演算結果をデジタル画像データに対するデジタル署名データとする。

【 0 0 5 7 】

図 4 は、第 1 の実施例の処理手順を説明するフローチャートである。以下、図

4に基づいて、ユーザの撮影指示からデジタル署名データの生成までの手順について説明する。

【0058】

ステップS401において、操作部208は、ある被写体の光学像を撮像するか否かを指示する。撮像が指示された場合、制御／演算部206はステップS402を実行する。

【0059】

ステップS402において、撮像部201は、被写体の光学像を電気信号に変換し、その電気信号を更に所定フォーマットのデジタル画像データを生成する。その後、デジタル画像データは、作業用メモリ202に格納される。

【0060】

ステップS403において、制御／演算部206（に含まれる画像処理回路211）は、作業用メモリ202に格納されたデジタル画像データを1画面分の静止画像毎に高能率符号化する。ここで、1つの静止画像を高能率符号化する方法として例えば、複数画素からなるブロック毎にDCT変換、量子化及び可変長符号化するDCT変換方式、そのブロック毎にウェーブレット変換、量子化及び可変長符号化するウェーブレット変換方式、JPEG方式、JBIG方式、MH方式、MMR方式、MPEG方式等を用いてもよい。尚、以下の実施例では、JPEG方式を用いて高能率符号化する場合について説明する。

【0061】

ステップS404において、制御／演算部206は、画像入力装置10の持つ固有の秘密情報をメモリ213から読み出す。

【0062】

ステップS405において、制御／演算部206（に含まれる演算回路212）は、上述の秘密情報と例えばJPEG方式で高能率符号化されたデジタル画像データ（以下、JPEGデータと称する）とを用いて、予め定められた規則に基づく所定の演算処理を行う。

【0063】

ここで、秘密情報と所定の演算処理とについて説明する。

【0064】

まず、秘密情報とは、画像入力機器10の製造時に設定される機器固有の情報であり、一般に公開されることのない情報である。この秘密情報は、外部から容易に入手することができないように制御／演算部206の内部に組み込まれている。以下、第1の実施例では、上述の秘密情報を例えば“11111111”として説明する。尚、この秘密情報は、画像検証装置20のもつ固有の秘密情報と共有できるものであればいかなるデータであってもよい。

【0065】

次に、上述の所定の演算処理について説明する。所定の演算処理とは、図5に示すように、あるJPEGデータ列から所定の位置のバイトデータを選択し、そのバイトデータと秘密情報とをビット毎に排他的論理和演算することによってそのバイトデータを別のデータに変換する処理のことである。ここで、所定の位置とは、JPEGデータ列上の任意の位置に設定することができるが、第1の実施例では最上位のバイトデータを演算対象とする。

【0066】

ステップS406において、制御／演算部206（に含まれる演算回路212）は、所定の演算処理の施されたJPEGデータをハッシュ関数を用いて演算し、デジタル署名データを生成する。

【0067】

ここで、ハッシュ関数について説明する。

【0068】

ハッシュ関数Hとは、任意のビット長のデジタルデータMから、一定のビット長となる出力hを生成する機能を持つ。この出力hは、ハッシュ値と呼ばれる（又は、デジタル署名、メッセージダイジェスト、デジタル指紋等とも呼ばれる）。通常、ハッシュ関数には、一方向性と衝突耐性が要求される。一方向性とは、ハッシュ値hが与えられた際に、 $h = H(M)$ となるデジタルデータMの算出が計算量的に困難であることを示す。又、衝突耐性とは、デジタルデータMが与えられた際に、 $H(M) = H(M')$ となるデジタルデータM' ($M \neq M'$)の算出および $H(M) = H(M')$ 且つ $M \neq M'$ となるデジタルデータ

M、M'の算出が計算量的に困難であることを示す。ハッシュ関数には、MD-2、MD-4、MD-5、SHA-1、RIPEMD-128、RIPEMD-160等の方式が知られている。第1の実施例では、MD-5方式を使用する例について説明する。尚、このMD-5方式を用いて生成されるデジタル署名データのビット長は128ビットとなる。

【0069】

ステップS407において、記録再生部203は、制御/演算部206にて生成されたデジタル署名データとそれに対応するデジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【0070】

尚、図4に示す一連の処理手順を制御するプログラムは、ROM207に格納されている。このプログラムは、制御/演算部206（に含まれる制御回路210）によって読み出され、ユーザの撮像指示毎に起動される。これにより、デジタル画像を撮像する毎にその画像に対応したデジタル署名データを生成することができる。

【0071】

以上説明したように、第1の実施例では、高能率符号化されたデジタル画像データと画像入力装置10の有する固有の秘密情報とを用いて所定の演算を行い、その演算結果をハッシュ関数演算することによってそのデジタル画像データのデジタル署名データを生成している。これにより、不正なユーザは秘密情報がわからない限り、デジタル画像データからデジタル署名データを生成することはできない。又、デジタル画像データに対する不正な処理（例えば、不正な合成、改竄）をデジタル署名データに反映させることもできない。又、デジタル画像データと共に得られたデジタル署名データから元のデータ（即ち、ハッシュ関数演算する前のデータ）を知ることができない。

【0072】

このような構成により第1の実施例では、デジタルデータの著作権を保護すると共に、そのデジタルデータに対する不正な処理を簡単な構成で、高速に検出することができる。又、上述のデジタル署名データを用いて、ある画像デー

タがどの画像入力装置にて撮像されたかを特定することもできる。

【0073】

尚、第1の実施例では、上述の秘密情報を画像入力装置10の製造時に設定された情報としたがそれに限るものではない。画像検証装置20の秘密情報と共有できるものであれば、乱数発生回路214が所定のアルゴリズムに基づいて生成したビット列でもよい。

【0074】

又、第1の実施例では、上述の所定の演算処理の一例として、JPEGデータのバイトデータと秘密情報とを排他的論理和演算する構成について説明したがそれに限るものではない。高能率符号化されたデジタル画像データの少なくとも一部に秘密情報を付加、合成、多重する処理で且つ逆演算可能な処理であればいかなる演算処理であってもよい。

【0075】

又、第1の実施例では、高能率符号化後のデジタル画像データを記録媒体内に格納する前にデジタル署名データを生成する手順について説明したがそれに限るものではない。例えば、高能率符号化後のデジタル画像データを一度記録媒体内に格納した後、そのデジタル画像データを外部へ出力する前に上述の手順でデジタル署名データを生成するようにしてもよい。つまり、画像入力装置10から外部へ出力される前に必ずデジタル署名データを生成する構成であれば、どのタイミングでデジタル署名データを生成してもよい。但し、デジタル画像データを取り外し可能な記録媒体に記憶する場合には、上述の手順でデジタル署名データを生成する。

【0076】

(第2の実施例)

第2の実施例では、第1の実施例に比べてより安全性の高いデジタル署名データを生成する手順について詳細に説明する。より具体的には、第1の実施例のハッシュ関数演算の際に、演算データをフィードバックし、攪乱するように構成する。

【0077】

図6は、第2の実施例の処理手順を説明するフローチャートである。以下、図6に基づいて、ユーザの撮影指示後からデジタル署名データを生成するまでの手順について説明する。

【0078】

ステップS601～S603の処理は、上述の第1の実施例のステップS401～S403と同様の処理としてその説明を省略する。

【0079】

ステップS604において、制御／演算部206（に含まれる乱数発生回路214）は、所定の情報（例えば、高能率符号化されたデジタル画像データのデータ量）を基にしてビット長 m の乱数 R を生成する。この乱数 R が第2の実施例の秘密情報である。

【0080】

次のステップS605～S606では、第2の実施例における所定の演算処理を説明する。

【0081】

ステップS605において、制御／演算部206（に含まれる演算回路212）は、図7に示すように、1画像分のJPEGデータを所定の大きさ、例えば128ビット長のブロック D_i （ $i=1, 2, 3 \dots N$ ）に分割する。ここで、 D_1 を最上位ブロックとする。ここで、JPEGデータの総量が128の倍数にならない場合、128の倍数になるようにするパディングする。例えば、図7に示すように最後のブロックに“000...000”を付加することが考えられる。

【0082】

ステップS606において、制御／演算部206（に含まれる演算回路212）は、上述の乱数 R と上述の N 個のブロックとを用いて以下に示す手順の演算を行う。

【0083】

まず、制御／演算部206は、図8に示すように、乱数 R のビット数を図7に示すブロック D_i の個数 N と同じとなるように処理する。例えば、 $m \geq N$ の場合

、最上位ビットから n ($n=N$) ビットまでのビット列を有効とし、それ以外のビット列を切り捨てる。又、 $m < N$ の場合、不足分のデータとして “111…111” を付加する。

【0084】

次に、制御／演算部 206 は、図 9 に示すように、各ブロック $D_1 \sim D_N$ と各乱数 $R_1 \sim R_n$ とで所定の演算を行う。具体的には、乱数 R のビット R_i とブロック D_i の最下位ビットとの間で排他的論理和演算を行い、その演算を $i=1 \sim n$ となるまで繰り返し行う。

【0085】

ここで、ステップ S606 の演算は、乱数 R_i とブロック D_i の最下位ビットとの間の排他的論理和演算としたがそれに限るものではない。各ブロック D_i の少なくとも一部に秘密情報（ビット長 m の乱数 R の一部）を付加、合成、多重する処理で且つ逆演算可能な処理であればいかなる演算処理であってもよい。

【0086】

ステップ S607 において、制御／演算部 206（に含まれる演算回路 212）は、ステップ S606 の出力に対してハッシュ関数演算を施し、デジタル署名データを生成する。尚、第 2 の実施例では、第 1 の実施例と同様に、MD-5 方式のハッシュ関数を用いる。従って、デジタル署名データのビット長は、128 ビットとなる。

【0087】

以下、ステップ S607 におけるハッシュ関数演算について説明する。

【0088】

制御／演算部 206 は、後述する 3 つの動作モードの何れか 1 つ又はこれらの組み合わせることによりハッシュ値 h を求める。何れの演算方法においても、演算データを攪乱しながらハッシュ値を求めるため、より安全性の高いデジタル署名データを生成することができる。又、何れの演算方法においても、前の演算の結果が次の演算の結果に反映されるため、各演算単位毎にデータの正当性を検証することもできる。

【0089】

①第1のモード

図10を用いて説明する。図10は、制御／演算部206の構成の一部を示す図である。

【0090】

図10において、演算回路212は、所定のビット単位でハッシュ関数演算を行うハッシュ関数演算回路1001と、ハッシュ関数演算回路1001の出力hの一部を記憶するレジスタ1002と、ステップS606の処理を実現する演算回路1003と、演算回路1003の出力とレジスタ1002の出力とを排他的論理和演算する演算回路1004とから構成されている。

【0091】

ハッシュ関数演算回路1001の出力である128ビットのハッシュ値hの一部は、レジスタ1002に入力される。レジスタ1002には、例えば、ハッシュ値hの上位64ビットが一時的に格納される。

【0092】

レジスタ1002に格納された64ビットデータは、次の演算対象（JPEGデータの一部）と排他的論理和演算され、その演算結果はハッシュ関数演算回路1001に供給される。

【0093】

最終的に、1 JPEGデータを複数のブロック単位毎に順次ハッシュ関数演算した結果が、128ビットのデジタル署名データとして出力される。

【0094】

ここで、最初の演算では、レジスタ1002に初期値を格納しておく必要がある。その初期値は、例えば図13に示すように、乱数Rの下位64ビットを用いることができる。

【0095】

尚、ブロックDiの大きさが64の倍数とならない場合には、例えば後述の第3のモードと組合せて余りのビット列を演算するように構成してもよい。

【0096】

②第2のモード

図11を用いて説明する。図11は、制御／演算部206の構成の一部を示す図である。

【0097】

図11において、演算回路212は、所定のビット単位でハッシュ関数演算を行うハッシュ関数演算回路1101と、ハッシュ関数演算回路1101に必要な入力値を供給するレジスタ1102と、ハッシュ関数演算回路1101の出力hを選択的に出力するセレクタ1103と、ステップS606の処理を実現する演算回路1104と、演算回路1104の出力とセレクタ1103の出力とを排他的論理和演算する演算回路1105とから構成されている。

【0098】

ハッシュ関数演算回路1101は、乱数発生回路214にて生成された秘密情報を初期値とするレジスタ1102の値を順次ハッシュ関数演算する。

【0099】

ハッシュ関数演算回路1101の出力である128ビットのハッシュ値hは、セレクタ1103に入力される。セレクタ1103は、128ビットのハッシュ値hの内、例えば下位Kビットをシフトして出力する。このKビットは、次にハッシュ関数演算されるデータとしてレジスタ1102に格納される。

【0100】

又、セレクタ1103から出力されたKビットは、演算回路1104の出力の一部と排他的論理和演算され、その結果が128ビットのデジタル署名データとなる。

【0101】

尚、最初のハッシュ関数演算に必要な初期値は、例えば図13に示すように、上述の乱数Rの下位64ビットを用いることができる。

【0102】

③第3のモード

図12を用いて説明する。図12は、制御／演算部206の構成の一部を示す

図である。

【0103】

図12において、演算回路212は、所定のビット単位でハッシュ関数演算を行うハッシュ関数演算回路1201と、ハッシュ関数演算回路1201に必要な入力値を供給するレジスタ1202と、ハッシュ関数演算回路1201の出力hを選択的に出力するセレクタ1203と、ステップS606の処理を実現する演算回路1204と、演算回路1204の出力とセレクタ1203の出力とを排他的論理和演算する演算回路1205とから構成されている。

【0104】

ハッシュ関数演算回路1201は、乱数発生回路214にて生成された秘密情報を初期値とするレジスタ1102の値を順次ハッシュ関数演算する。

【0105】

ハッシュ関数演算回路1201の出力である128ビットのハッシュ値hは、セレクタ1203に入力される。セレクタ1203は、128ビットのハッシュ値hの内、例えば下位Kビットをシフトして出力する。このKビットは、次の演算対象（JPEGデータの一部）と排他的論理和演算され、その演算結果の一部は再びレジスタ1202に格納される。

【0106】

最終的に、1 JPEGデータを複数のブロック単位毎に順次ハッシュ関数演算した結果が、128ビットのデジタル署名データとして出力される。

【0107】

尚、最初のハッシュ関数演算に必要な初期値は、例えば図13に示すように、上述の乱数Rの下位64ビットを用いることができる。

【0108】

ステップS608において、記録再生部203は、制御／演算部206にて生成されたデジタル署名データとそれに対応するデジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【0109】

尚、図6に示す一連の処理手順を制御するプログラムは、ROM207に格納

されている。このプログラムは、制御／演算部 2 0 6（に含まれる制御回路 2 1 0）によって読み出され、ユーザの撮像指示毎に起動される。

【0 1 1 0】

以上のように第 2 の実施例では、ある長さの乱数を生成し、その乱数と高能率符号化されたデジタル画像データとを用いて所定の演算処理を行い、その演算結果をハッシュ関数演算してデジタル署名データを生成している。このような構成により第 2 の実施例では、デジタルデータの著作権を保護すると共に、そのデジタルデータに対する不正な処理を簡単な構成で、高速に検出することができる。

【0 1 1 1】

又、第 2 の実施例では、ハッシュ関数演算を上述の動作モードの 1 つまたは複数を組み合わせて実現することにより、第 1 の実施例に比べてより安全性の高いデジタル署名データ生成アルゴリズムを提供することができる。

【0 1 1 2】

又、第 2 の実施例では、上述のデジタル署名データを用いて、ある画像データがどの画像入力装置にて撮像されたかを特定することもできる。

【0 1 1 3】

（第 3 の実施例）

第 1、第 2 の実施例では、ハッシュ関数を用いてデジタル署名データを生成する手順について説明した。

【0 1 1 4】

第 3 の実施例では、ハッシュ関数ではなく共通鍵暗号処理を用いてデジタル署名データを生成する手順について詳細に説明する。

【0 1 1 5】

図 1 4 は、第 3 の実施例の処理手順を説明するフローチャートである。以下、図 1 4 に基づいて、ユーザの撮影指示後からデジタル署名データを生成するまでの手順について説明する。

【0 1 1 6】

ステップ S 1 4 0 1 ～ S 1 4 0 3 の処理は、上述の第 1 の実施例のステップ S

401～S403と同様の処理としてその説明を省略する。

【0117】

ステップS1404において、制御／演算部206は、画像入力装置10の持つ固有の秘密情報をメモリ213から読み出す。第3の実施例では、“1111…1111”（128ビット）を秘密情報とする。尚、この秘密情報は、一般に公開されず且つ画像検証装置20の持つ固有の秘密情報と共有できるものであればいかなるデータであってもよい。

【0118】

ステップS1405において、制御／演算部206（に含まれる演算回路212）は、作業用メモリ202に保持されたJPEGデータを共通鍵暗号方式に基づいて暗号化する。

【0119】

ここで、共通鍵暗号方式には現在様々なものが提案されているが、例えば第3の実施例ではDES方式を用いる。DES方式を使用する場合、暗号鍵のビット長は56ビットであるので、図15に示すように秘密情報の上位56ビットを暗号鍵とすることが考えられる。ここで、この暗号鍵のビット長は、使用する共通鍵暗号方式の種類によって異なるものである。従って、FEAL-nX, MITSY, IDEAを使用する場合、暗号鍵は128ビットであるので秘密情報の上位128ビットを暗号鍵としてもよい。又、FEAL-n, MULTI2を使用する場合、暗号鍵は64ビットであるので秘密情報の上位64ビットを暗号鍵としてもよい。

【0120】

以下、ステップS1405における暗号化処理について説明する。

【0121】

制御／演算部206は、後述する3つの動作モード（即ち、CBCモード、CFBモード、OFBモード）の何れか1つ又はこれらの組み合わせることによりJPEGデータを上述の暗号鍵で暗号化する。何れの動作モードにおいても、入力データをデータ量に関わらず暗号化することができ、且つ入力データを攪乱しながら暗号化することができるのでより安全性の高い暗号化処理を実現できる。

【0122】

①CBC (Cipher Block Chaining) モード

図16を用いて説明する。図16は、制御／演算部206の一部（即ち、演算回路212）を示す図である。

【0123】

図16において、演算回路212は、64ビット単位で暗号化を行う暗号化回路1601と、暗号化回路1601の出力を一時的に保持するレジスタ1602と、JPEGデータとレジスタ1602の出力とを排他的論理和演算する演算回路1603とから構成されている。

【0124】

暗号化回路1601は、64ビット単位で暗号化を行う。従って、暗号化回路1601は、JPEGデータを64ビットからなるブロック毎に暗号化する。暗号化回路1601の出力はレジスタ1602に一時的に格納される。レジスタ1602に格納された64ビットデータは、次のブロックと排他的論理和演算され、その演算結果は暗号化回路1601に供給される。最終的に、全てのブロックを暗号化した結果が暗号データとして出力される。

【0125】

ここで、最初のブロックの暗号化では、レジスタ1602に初期値を格納しておく必要がある。その初期値は、例えばIV (Initial Vector) と呼ばれる初期値を使用する。このIVは、暗号化処理と復号処理において同じ値を供給する必要がある。又、例えば、図15に示すように、秘密情報の下位64ビットを用いることもできる。

【0126】

尚、ブロックの大きさが64の倍数とならない場合には、例えば後述のOFBモードと組合せて余りのビット列を暗号化するように構成してもよい。

【0127】

②CFB (Cipher Feedback) モード

図17を用いて説明する。図17は、制御／演算部206の一部（即ち、演算回路212）を示す図である。CFBモードでは、暗号化側と復号側とで同じ長

さのビット列を暗号化が可能な場合に利用される。

【0128】

図17において、演算回路212は、64ビット単位で暗号化を行う暗号化回路1701と、暗号化回路1701に必要な入力値を供給するレジスタ1702と、暗号化回路1701の出力を選択的に出力するセクタ1703と、JPEGデータとセクタ1703の出力とを排他的論理和演算する演算回路1704とから構成されている。

【0129】

暗号化回路1701は、64ビット単位で暗号化を行う。従って、暗号化回路1701は、レジスタ1702に格納された64ビットデータを順次暗号化する。暗号化回路1701の出力は、セクタ1703に入力される。セクタ1703は、例えば下位Kビットをシフトして出力する。このKビットは、次に暗号化されるデータとしてレジスタ1702に格納される。セクタ1703から出力されたKビットは、JPEGデータの一部（64ビットのブロック）と排他的論理和演算され、その結果が暗号データとなる。

【0130】

ここで、最初の暗号化に必要な初期値は、例えば図15に示しように、上述の秘密情報の下位64ビットを用いることができる。

【0131】

③OFB (Output Feedback) モード

図18を用いて説明する。図18は、制御／演算部206の一部（即ち、演算回路212）を示す図である。OFBモードは、CFBモードと同様に、暗号化側と復号側とで同じ長さのビット列を暗号化が可能な場合に利用される。

【0132】

図18において、演算回路212は、64ビット単位で暗号化を行う暗号化回路1801と、暗号化回路1801に必要な入力値を供給するレジスタ1802と、暗号化回路1801の出力を選択的に出力するセクタ1803と、JPEGデータとセクタ1803の出力とを排他的論理和演算する演算回路1804とから構成されている。

【0133】

暗号化回路1801は、64ビット単位で暗号化を行う。従って、暗号化回路1801は、レジスタ1802に格納された64ビットデータを順次暗号化する。暗号化回路1801の出力は、セレクタ1803に入力される。セレクタ1803は、例えば下位Kビットをシフトして出力する。セレクタ1803から出力されたKビットは、JPEGデータの一部（64ビットのブロック）と排他的論理和演算され、その結果が暗号データとなる。ここで、暗号データの一部（Kビット）は、再びレジスタ1802に格納される。

【0134】

ここで、最初のハッシュ関数演算に必要な初期値は、例えば図15に示しように、上述の秘密情報の下位64ビットを用いることができる。

【0135】

ステップS1406において、制御／演算部206（に含まれる演算回路212）は、ステップS1405にて生成された暗号データから特定のビット列をデジタル署名データとして抽出する。例えば、上述の暗号データの下位128ビットをデジタル署名データとすることができる。

【0136】

ステップS1407において、記録再生部203は、制御／演算部206（に含まれる演算回路212）にて生成されたデジタル署名データとそれに対応するデジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【0137】

尚、図14に示す一連の処理手順を制御するプログラムは、ROM207に格納されている。このプログラムは、制御／演算部206（に含まれる制御回路210）によって読み出され、ユーザの撮像指示毎に起動される。

【0138】

以上のように第3の実施例では、画像入力装置10と画像検証装置20とで共有される秘密情報の一部からなる暗号鍵を用いて、高能率符号化されたデジタル画像データを暗号化し、その結果生成された暗号データの一部をデジタル署名データとする構成について説明した。このような構成により第3の実施例では

、デジタルデータの著作権を保護すると共に、第1の実施例に比べてより安全性の高いデジタル署名データ生成アルゴリズムを提供することができる。

【0139】

又、第3の実施例では、上述のデジタル署名データを用いて、あるデジタル画像データがどの画像入力装置にて撮像されたかを特定することもできる。

【0140】

尚、第3の実施例では、秘密情報を“1111…1111”（128ビット）としたがこれに限るものではない。例えば、乱数発生回路214が所定のアルゴリズムに基づいて発生させた乱数とすることも可能である。但し、この秘密情報は画像検証装置20と共有される。

【0141】

（第4の実施例）

第3の実施例では、ハッシュ関数演算ではなく共通鍵暗号演算を用いてデジタル署名データを生成する手順について説明した。

【0142】

第4の実施例では、共通鍵暗号演算の前に所定の演算処理（例えば、ビット挿入を含む逆演算可能な演算処理）を行い、その演算結果を暗号化し、その暗号結果からデジタル署名データを生成する手順について説明する。

【0143】

図19は、第4の実施例の処理手順を説明するフローチャートである。以下、図19に基づいて、ユーザの撮影指示後からデジタル署名データを生成するまでの手順について説明する。

【0144】

ステップS1901～S1903の処理は、上述の第1の実施例のステップS401～S403と同様の処理としてその説明を省略する。

【0145】

ステップS1904～S1906の処理は、上述の第2の実施例のステップS604～S606と同様の処理（即ち、秘密情報である乱数RのビットR_iとJPEGデータのブロックD_iとを用いた排他的論理和演算）としてその説明を省

略する。

【0146】

ここで、ステップS1906の演算は、上述のステップS606と同様に、乱数 R_i とブロック D_i の最下位ビットとの間の排他的論理和演算としたがそれに限るものではない。各ブロック D_i の少なくとも一部に秘密情報（ビット長 m の乱数 R の一部）を付加、合成、多重する処理で且つ逆演算可能な処理であればいかなる演算処理であってもよい。

【0147】

ステップS1907において、制御／演算部206（に含まれる演算回路212）は、ステップS1906の出力に対して共通鍵暗号化方式に従った暗号化処理を施す。ここで、制御／演算部206は、第3の実施例と同様に、DES方式を利用するものとし、その暗号化処理に必要な暗号鍵は、ステップS1904で生成した秘密情報（即ち、乱数 R ）の上位56ビットとする（図20参照）。

【0148】

以下、ステップS1907における暗号化処理について説明する。

【0149】

制御／演算部206は、上述した3つの動作モード（即ち、CBCモード、CFBモード、OFBモード）の何れか1つ又はこれらの組み合わせることにより、乱数 R のビット R_i とJPEGデータのブロック D_i との排他的論理和演算の結果を上述の暗号鍵を用いて順次暗号化する。何れの動作モードにおいても、入力データをデータ量に関わらず暗号化することができ、且つ入力データを攪乱しながら暗号化することができるのでより安全性の高い暗号化処理を実現できる。

【0150】

尚、これらの動作モードにおいて、最初のブロックの暗号化では、上述のように初期値が必要であるが、例えばその初期値を図20に示すように、秘密情報（即ち、乱数 R ）の下位64ビットとすることができる。

【0151】

又、CBCモードにおいて、ブロック D_i の大きさが64の倍数とならない場合には、例えば後述のOFBモードと組合せて余りのビット列を暗号化するよう

に構成してもよい。

【0152】

ステップS1908において、制御／演算部206（に含まれる演算回路212）は、ステップS1907にて生成された暗号データから特定のビット列をデジタル署名データとして抽出する。例えば、上述の暗号データの下位128ビットをデジタル署名データとすることができる。

【0153】

ステップS1909において、記録再生部203は、制御／演算部206（に含まれる演算回路212）にて生成されたデジタル署名データとそれに対応するデジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【0154】

尚、図19に示す一連の処理手順を制御するプログラムは、ROM207に格納されている。このプログラムは、制御／演算部206（に含まれる制御回路210）によって読み出され、ユーザの撮像指示毎に起動される。

【0155】

以上のように第4の実施例では、ある長さの乱数を発生させ、その乱数と高エネルギー符号化されたデジタル画像データとをあらかじめ決められた規則に従った演算を行い、その演算結果を共通鍵暗号方式により暗号化し、その結果得られた暗号データの一部をデジタル署名データとしている。このような構成により第4の実施例では、デジタルデータの著作権を保護すると共に、第1、第2の実施例に比べてより安全性の高いデジタル署名データ生成アルゴリズムを提供することができる。

【0156】

又、第4の実施例では、共通鍵暗号化方式による暗号化処理を上述の動作モードの1つまたは複数を組み合わせて実現することにより、第1、第2の実施例に比べてより安全性の高いデジタル署名データ生成アルゴリズムを提供することができる。

【0157】

又、第4の実施例では、上述のデジタル署名データを用いて、あるディジタ

ル画像データがどの画像入力装置にて撮像されたかを特定することもできる。

【0158】

(第5の実施例)

第1～第4の実施例では、画像入力装置10が、画像入力装置10自体の持つ固有の秘密情報に基づいてデジタル署名データを生成する構成について説明した。このような構成により第1～第4の実施例では、デジタル署名データを用いて、ある画像データがどの画像入力装置にて撮像されたものであるかを特定することができる。

【0159】

これに対して、第5の実施例では、外部装置（例えば、ICカード等）を画像入力装置10に接続し、この外部装置の持つ固有の秘密情報に基づいてデジタル署名データを生成する構成について説明する。ここで、外部機器の持つ秘密情報は、例えば、画像入力装置10を識別するためのID情報、画像入力装置10を使用するユーザを識別するためのID情報とすることができる。このように構成することにより第5の実施例では、デジタル署名データを用いて、ある画像データがどの外部機器を使用して撮像されたものか、或いはどのユーザによって撮像されたものであるかを特定することができる。

【0160】

図21は、第5の実施例の処理手順を説明するフローチャートである。以下、図21に基づいて、外部装置の接続からデジタル署名データの生成までの手順について説明する。

【0161】

ステップS2101において、画像入力装置10の制御/演算処理部206は、外部I/F部205に外部装置40が接続されているか否かを検出する。

【0162】

ステップS2102において、画像入力装置10の制御/演算処理部206及び外部装置40の制御/演算処理部306とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。

【0163】

ここで、図22を用いて画像入力装置10と外部装置40との相互認証処理について説明する。

【0164】

画像入力装置10は、乱数発生回路214を用いて認証用の乱数aを発生させ、その乱数aを外部I/F部205を介して外部装置40に送信する。

【0165】

次に外部装置40の暗号化回路43は、認証用の暗号鍵を用いて乱数aをAに変換し、その暗号データAを外部I/F部41を介して画像入力装置10へ送信する。

【0166】

又、画像入力装置10の暗号化回路2201は、乱数aを認証用の暗号鍵を用いてA'に変換する。比較回路2202は、その暗号データA'を外部装置40から送信された暗号データAと比較し、それらが一致すれば外部装置40を認証する。

【0167】

同様にして、外部装置40は、乱数発生回路42を用いて認証用の乱数bを発生させ、その乱数bを外部I/F部205を介して画像入力装置10に送信する。

【0168】

次に画像入力装置10の暗号化回路2201は、認証用の暗号鍵を用いて乱数bをBに変換し、その暗号データBを外部I/F部205を介して外部装置40へ送信する。

【0169】

又、外部装置40の暗号化回路43は、乱数bを認証用の暗号鍵を用いてB'に変換する。比較回路44は、その暗号データB'を画像入力装置10から送信された暗号データBと比較し、それらが一致すれば画像入力装置10を認証する。

【0170】

双方が正常に認証された場合、外部装置40は、メモリ45に格納された秘密情報を外部I/F部41を介して画像入力装置10に送信する。

【0171】

ステップS2103～S2105の処理は、上述の第1の実施例のステップS401～S403と同様の処理としてその説明を省略する。

【0172】

ステップS2106において、制御/演算部206は、外部I/F部205を介して入力された外部装置40の持つ固有の秘密情報をメモリ213に格納し、デジタル署名データの生成に必要な秘密情報として管理する。

【0173】

ステップS2107において、制御/演算部206（に含まれる演算回路212）は、上述の秘密情報と例えばJPEG方式で高能率符号化されたデジタル画像データ（以下、JPEGデータと称する）とを用いて、予め定められた規則に基づく所定の演算処理を行う。ここで、演算回路212は、第1の実施例のステップS405と同様の演算処理を行う。

【0174】

ステップS2108において、制御/演算部206（に含まれる演算回路212）は、ステップS2107の演算結果をハッシュ関数演算し、その結果からデジタル署名データを生成する。ここで、演算回路212は、第1の実施例のステップS406と同様の演算処理を行う。

【0175】

ステップS2109において、記録再生部203は、制御/演算部206にて生成されたデジタル署名データとそれに対応するデジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【0176】

尚、図21に示す一連の処理手順を制御するプログラムは、ROM207に格納されている。このプログラムは、制御/演算部206（に含まれる制御回路210）によって読み出され、ユーザの撮像指示毎に起動される。これにより、デ

ィジタル画像を撮像する毎にその画像に対応したディジタル署名データを生成することができる。

【0177】

以上説明したように、第5の実施例では、画像入力装置10の高能率符号化されたディジタル画像データと画像入力装置10と接続された外部装置40の有する秘密情報とを用いて所定の演算を行い、その演算結果をハッシュ関数演算することによってそのディジタル画像データのディジタル署名データを生成している。これにより、不正なユーザはこの秘密情報がわからない限り、ディジタル画像データからディジタル署名データを生成することはできない。又、ディジタル画像データに対する不正な処理（例えば、不正な合成、改竄）をディジタル署名データに反映させることもできない。又、ディジタル画像データと共に得られたディジタル署名データから元のデータ（即ち、ハッシュ関数演算する前のデータ）を知ることもしない。

【0178】

このような構成により第5の実施例では、ディジタルデータの著作権を保護すると共に、そのディジタルデータに対する不正な処理を検出するための署名データを簡単な構成で、高速に生成することができる。又、上述のディジタル署名データを用いて、ある画像データがどの外部機器或いはどのユーザにて撮像されたかを特定することもできる。

【0179】

尚、第5の実施例では、ディジタル署名データを生成するための演算処理を第1の実施例と同様の演算処理としたがそれに限るものではない。上述の第2～第4の実施例と同様の演算処理を適用することも可能である。

【0180】

（第6の実施例）

第5の実施例では、画像入力装置10に外部装置40を接続し、この外部装置40の持つ固有の秘密情報に基づいてディジタル署名データを生成する構成について説明した。

【0181】

これに対して、第6の実施例では、画像入力装置10を外部装置40に接続し、この外部装置40の持つ固有の秘密情報と画像入力装置10の持つ固有の秘密情報とに基づいてデジタル署名データを生成する構成について説明する。このように構成することにより第6の実施例では、デジタル署名データを用いて、ある画像データがどの外部機器と接続されたどの画像入力装置によって撮像されたものか、或いはどのユーザが使用するどの画像入力装置によって撮像されたものであるかを特定することができる。

【0182】

以下、図21を用いて第6の実施例の処理手順を説明する。

【0183】

ステップS2101において、画像入力装置10の制御/演算処理部206は、外部I/F部205に外部装置40が接続されているか否かを検出する。

【0184】

ステップS2102において、画像入力装置10の制御/演算処理部206及び外部装置40の制御/演算処理部306とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。相互認証処理の一例を図22に示す。

【0185】

ステップS2103～S2105の処理は、上述の第1の実施例のステップS401～S403と同様の処理としてその説明を省略する。

【0186】

ステップS2106において、制御/演算部206は、画像入力装置10の持つ固有の秘密情報をメモリ213から読み出し、外部装置40の持つ固有の秘密情報を外部I/F部205を介して入力する。そして、これらの秘密情報を結合させ、新しい秘密情報を生成する。

【0187】

ここで、画像入力装置10の秘密情報を例えば“1111”とし、外部装置40の秘密情報を例えば“0000”とすると、新たに生成される秘密情報は、例えば“11110000”となる。尚、第6の実施例では、2つの秘密情報を単

に結合することにより新たな秘密情報を生成したが、これら2つの秘密情報のみに基づいて生成されるのであれば、どのような演算であってもよい。又、これら2つの秘密情報は、画像検証装置20の持つ固有の秘密情報と共有できるものであればいかなるデータであってもよい。

【0188】

ステップS2107において、制御／演算部206（に含まれる演算回路212）は、上述の秘密情報と例えばJPG方式で高能率符号化されたデジタル画像データ（以下、JPGデータと称する）とを用いて、予め定められた規則に基づく所定の演算処理を行う。ここで、演算回路212は、第1の実施例のステップS405と同様の演算処理を行う。

【0189】

ステップS2108において、制御／演算部206（に含まれる演算回路212）は、ステップS2107の演算結果をハッシュ関数演算し、その結果からデジタル署名データを生成する。ここで、演算回路212は、第1の実施例のステップS406と同様の演算処理を行う。

【0190】

ステップS2109において、記録再生部203は、制御／演算部206にて生成されたデジタル署名データとそれに対応するデジタル画像データとを一組として、取り外し可能な記録媒体に記録する。

【0191】

尚、図21に示す一連の処理手順を制御するプログラムは、ROM207に格納されている。このプログラムは、制御／演算部206（に含まれる制御回路210）によって読み出され、ユーザの撮像指示毎に起動される。これにより、デジタル画像を撮像する毎にその画像に対応したデジタル署名データを生成することができる。

【0192】

以上説明したように、第6の実施例では、画像入力装置10の高能率符号化されたデジタル画像データと、画像入力装置10の有する秘密情報と、外部装置40の有する秘密情報とを用いて所定の演算を行い、その演算結果をハッシュ関

数演算することによってそのデジタル画像データのデジタル署名データを生成している。

【0193】

このような構成により第6の実施例では、デジタルデータの著作権を保護すると共に、そのデジタルデータに対する不正な処理を検出するための署名データを簡単な構成で、高速に生成することができる。又、上述のデジタル署名データを用いて、ある画像データがどの外部機器と接続された画像入力装置或いはどのユーザによって使用された画像入力装置にて撮像されたかを特定することもできる。

【0194】

尚、第6の実施例では、デジタル署名データを生成するための演算処理を第1の実施例と同様の演算処理としたがそれに限るものではない。上述の第2～第4の実施例と同様の演算処理を適用することも可能である。

【0195】

(第7の実施例)

第7の実施例では、画像検証装置20が、第1の実施例に基づいて生成されたデジタル署名データを用いて、JPEGデータの正当性を確認する構成について説明する。

【0196】

具体的に、画像検証装置20は、外部入力されたJPEGデータと、画像入力装置10と画像検証装置20とで共有する秘密情報とに基づいて所定の演算を行い、その演算結果と該JPEGデータとセットで入力されたデジタル署名データとを比較し、その比較結果に基づいて該JPEGデータの正当性を検証する。

【0197】

図23は、第7の実施例の処理手順の一例を説明するフローチャートである。以下、図23に基づいて、デジタル画像データの入力からその検証までの手順について説明する。

【0198】

ステップS2301において、外部I/F部301は、画像入力装置10から

送信された1画像分の高能率符号化データ（例えば、J P E G方式で圧縮符号化されたJ P E Gデータ）とそれに対応するデジタル署名データとを入力し、それらを画像検証装置20内の記録媒体（例えば、作業用メモリ302）に格納する。

【0199】

ステップS2302において、操作部306は、所望のJ P E Gデータを選択し、そのJ P E Gデータの正当性を検証するか否かを選択する。検証が指示された場合、制御／演算部206はステップS2303を実行する。

【0200】

ステップS2303において、制御／演算部303は、メモリ313から秘密情報を読み出す。ここで、この秘密情報は、第1の実施例の画像入力装置10と本実施例の画像検証装置20とで共有している秘密情報である。従って、本実施例の秘密情報は、第1の実施例と同様に“11111111”とすることができる。尚、この秘密情報は、読み出し専用の記録媒体等の中に保存され、外部からその情報を入手できないように管理されている。

【0201】

ステップS2304において、制御／演算部303（に含まれる演算回路312）は、上述の秘密情報と選択されたJ P E Gデータとを用いて、第1の実施例のステップS405と同様の演算を行う。つまり、J P E Gデータの最上位バイトと秘密情報とをビット毎に排他的論理和演算する。

【0202】

ステップS2305において、制御／演算部303（に含まれる演算回路312）は、ステップS2304の演算結果に対してハッシュ関数演算を行う。ここでは、第1の実施例と同様のハッシュ関数が使用される。

【0203】

ステップS2306において、制御／演算部303（に含まれる演算回路312）は、ステップS2305の演算結果と、選択されたJ P E Gデータとセットで入力されたデジタル署名データを比較する。比較の結果、これらのデータが一致した場合には、J P E Gデータを正当なものと判断し、一致しなかった場合

には、J P E Gデータに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【0204】

ステップS2307において、表示部304は、ステップS2305の比較結果が一致した場合、選択されたJ P E Gデータが正常で、不正な処理の施されていないことを示す表示画像或いはメッセージを表示する。又、この比較結果が一致しなかった場合、不正な処理を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したJ P E Gデータの正当性を視覚的に分かり易く認識することができる。

【0205】

尚、図23に示す一連の処理手順を制御するプログラムは、ROM305に格納されている。このプログラムは、制御／演算部303（に含まれる制御回路312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0206】

以上の手順により、選択されたJ P E Gデータの正当性を確認した場合、ユーザは、操作部306を操作し、該J P E Gデータのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路310は各処理回路を制御し、該J P E Gデータを廃棄することもできる。

【0207】

以上説明したように、第7の実施例では、第1の実施例の画像入力装置10にて撮像され、高能率符号化されたデジタル画像データの正当性を簡単な構成で、高速に確認することができる。

【0208】

（第8の実施例）

第8の実施例では、画像検証装置20が、第2の実施例に基づいて生成されたデジタル署名データを用いて、J P E Gデータの正当性を確認する構成について説明する。

【0209】

図24は、第8の実施例の処理手順の一例を説明するフローチャートである。

以下、図24に基づいて、デジタル画像データの入力からその検証までの手順について説明する。

【0210】

ステップS2401、S2402の処理は、上述の第7の実施例のステップS2301、S2302と同様の処理としてその説明を省略する。

【0211】

ステップS2403において、制御／演算部303（に含まれる乱数発生回路）は、選択されたJPEGデータのデータ量を基にしてビット長 m の乱数 R （即ち、秘密情報）を発生させる。乱数 R を発生されるためのプログラムは、ROM305に格納されている。このプログラムは、第2の実施例の画像入力装置10の保持するプログラムと同様であり、乱数 R は、第2の実施例の乱数 R と同様である。尚、このプログラム及び乱数 R は、外部からその情報を入手できないように管理されている。

【0212】

ステップS2404において、制御／演算部303（に含まれる演算回路312）は、図7に示すように、選択されたJPEGデータを128ビットのブロック D_i （ $i=1\sim n$ ）に分割し、1ブロックのデータ量が128ビットにならない分については“000...000”をパディングする。尚、ステップS2404の処理は、第2の実施例のステップS605と同様の処理である。

【0213】

ステップS2405において、制御／演算部303（に含まれる演算回路312）は、上述の乱数 R と上述の N 個のブロックとを用いて第2の実施例のステップS606と同様の演算処理を行う。つまり、乱数 R のビット R_i とブロック D_i の最下位ビットとの間の排他的論理和演算を、 $i=1\sim n$ となるまで繰り返す。

【0214】

ステップS2406において、制御／演算部303（に含まれる演算回路312）は、ステップS2405の演算結果に対してハッシュ関数演算を行う。ここでは、第2の実施例と同様のハッシュ関数が使用される。

【0215】

ステップS2407において、制御／演算部303（に含まれる演算回路312）は、ステップS2406の演算結果と、選択されたJPEGデータとセットで入力されたデジタル署名データとを比較する。比較の結果、これらのデータが一致した場合には、JPEGデータを正当なものと判断し、一致しなかった場合には、JPEGデータに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【0216】

ステップS2408において、表示部304は、ステップS2407の比較結果、即ち不正な処理の有無を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したJPEGデータの正当性を視覚的に分かり易く認識することができる。

【0217】

尚、図24に示す一連の処理手順を制御するプログラムは、ROM305に格納されている。このプログラムは、制御／演算部303（に含まれる制御回路312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0218】

以上の手順により、選択されたJPEGデータの正当性を確認した場合、ユーザは、操作部306を操作し、該JPEGデータのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路310は各処理回路を制御し、該JPEGデータを廃棄することもできる。

【0219】

以上説明したように、第8の実施例では、第2の実施例の画像入力装置10にて撮像され、高能率符号化されたデジタル画像データの正当性を簡単な構成で、高速に確認することができる。

【0220】

（第9の実施例）

第9の実施例では、画像検証装置20が、第3の実施例に基づいて生成されたデジタル署名データを用いて、JPEGデータの正当性を確認する構成につい

て説明する。

【0221】

図25は、第9の実施例の処理手順の一例を説明するフローチャートである。以下、図25に基づいて、デジタル画像データの入力からその検証までの手順について説明する。

【0222】

ステップS2501、S2502の処理は、上述の第7の実施例のステップS2301、S2302と同様の処理としてその説明を省略する。

【0223】

ステップS2503において、制御／演算部303は、メモリ313から秘密情報を読み出す。ここで、この秘密情報は、第3の実施例の画像入力装置10と本実施例の画像検証装置20とで共有している秘密情報である。従って、本実施例の秘密情報は、第3の実施例と同様に“11111111”とすることができる。尚、この秘密情報は、読み出し専用の記録媒体等の中に保存され、外部からその情報を入手できないように管理されている。

【0224】

ステップS2504において、制御／演算部303（に含まれる演算回路312）は、第3の実施例のステップS1405と同様に、選択されたJPEGデータを共通鍵暗号方式に基づいて暗号化する。ここで、JPEGデータの暗号化使用される関数は、第3の実施例と同様の関数である。例えば、上述のCBCモードとOFBモードとを組み合わせて使用する場合、CBCモードを用いて入力データを64ビット単位に暗号化し、余りのデータをOFBモードにて暗号化する。

【0225】

ステップS2505において、制御／演算部303（に含まれる演算回路312）は、ステップS2504にて生成された暗号データから特定のビット列を抽出する。例えば、第3の実施例と同様に、上述の暗号データの下位128ビットを抽出する。

【0226】

ステップS2506において、制御／演算部303（に含まれる演算回路312）は、ステップS2505の抽出結果と、選択されたJPEGデータとセットで入力されたデジタル署名データとを比較する。比較の結果、これらのデータが一致した場合には、JPEGデータを正当なものと判断し、一致しなかった場合には、JPEGデータに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【0227】

ステップS2507において、表示部304は、ステップS2506の比較結果、即ち不正な処理の有無を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したJPEGデータの正当性を視覚的に分かり易く認識することができる。

【0228】

尚、図25に示す一連の処理手順を制御するプログラムは、ROM305に格納されている。このプログラムは、制御／演算部303（に含まれる制御回路312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0229】

以上の手順により、選択されたJPEGデータの正当性を確認した場合、ユーザは、操作部306を操作し、該JPEGデータのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路310は各処理回路を制御し、該JPEGデータを廃棄することもできる。

【0230】

以上説明したように、第9の実施例では、第3の実施例の画像入力装置10にて撮像され、高能率符号化されたデジタル画像データの正当性を簡単な構成で、高速に確認することができる。

【0231】

（第10の実施例）

第10の実施例では、画像検証装置20が、第4の実施例に基づいて生成されたデジタル署名データを用いて、JPEGデータの正当性を確認する構成につ

いて説明する。

【0232】

図26は、第10の実施例の処理手順の一例を説明するフローチャートである。以下、図26に基づいて、デジタル画像データの入力からその検証までの手順について説明する。

【0233】

ステップS2601、S2602の処理は、上述の第7の実施例のステップS2301、S2302と同様の処理としてその説明を省略する。

【0234】

ステップS2603～S2605の処理は、上述の第8の実施例のステップS2403～S2405と同様の処理としてその説明を省略する。

【0235】

ステップS2606において、制御／演算部303（に含まれる演算回路312）は、第4の実施例のステップS1907と同様に、選択されたJPEGデータを共通鍵暗号方式に基づいて暗号化する。ここで、JPEGデータの暗号化使用される関数は、第4の実施例と同様の関数である。

【0236】

ステップS2607において、制御／演算部303（に含まれる演算回路312）は、ステップS2606にて生成された暗号データから特定のビット列を抽出する。例えば、第3の実施例と同様に、上述の暗号データの下位128ビットを抽出する。

【0237】

ステップS2608において、制御／演算部303（に含まれる演算回路312）は、ステップS2607の抽出結果と、選択されたJPEGデータとセットで入力されたデジタル署名データとを比較する。比較の結果、これらのデータが一致した場合には、JPEGデータを正当なものと判断し、一致しなかった場合には、JPEGデータに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【0238】

ステップS2609において、表示部304は、ステップS2608の比較結果、即ち不正な処理の有無を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したJPEGデータの正当性を視覚的に分かり易く認識することができる。

【0239】

尚、図26に示す一連の処理手順を制御するプログラムは、ROM305に格納されている。このプログラムは、制御/演算部303（に含まれる制御回路312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0240】

以上の手順により、選択されたJPEGデータの正当性を確認した場合、ユーザは、操作部306を操作し、該JPEGデータのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路310は各処理回路を制御し、該JPEGデータを廃棄することもできる。

【0241】

以上説明したように、第10の実施例では、第4の実施例の画像入力装置10にて撮像され、高能率符号化されたデジタル画像データの正当性を簡単な構成で、高速に確認することができる。

【0242】

（第11の実施例）

第11の実施例では、画像検証装置20が、第5の実施例に基づいて生成されたデジタル署名データを用いて、JPEGデータの正当性を確認する構成について説明する。

【0243】

図27は、第10の実施例の処理手順の一例を説明するフローチャートである。以下、図27に基づいて、デジタル画像データの入力からその検証までの手順について説明する。

【0244】

ステップS2701において、画像検証装置20の制御/演算処理部303は

、外部 I/F 部 301 に外部装置 40 が接続されているか否かを検出する。

【0245】

ステップ S2702 において、画像検証装置 20 の制御/演算処理部 303 及び外部装置 40 の制御/演算処理部 306 とは、相互認証を行い、互いに正当なものであるかどうかをチェックする。この相互認証は、第 5 の実施例に示す図 2 と同様の手順で実行される。

【0246】

ステップ S2703、S2704 の処理は、上述の第 7 の実施例のステップ S2301、S2302 と同様の処理としてその説明を省略する。

【0247】

ステップ S2705 において、制御/演算部 303 は、外部 I/F 部 301 を介して入力された外部装置 40 の持つ固有の秘密情報をメモリ 313 に格納し、デジタル署名データの生成に必要な秘密情報として管理する。

【0248】

ステップ S2706 において、制御/演算部 303（に含まれる演算回路 312）は、上述の秘密情報と JPEG データとを用いて、予め定められた規則に基づく所定の演算処理を行う。ここで、演算回路 312 は、第 7 の実施例のステップ S2304 と同様の演算処理を行う。

【0249】

ステップ S2707 において、制御/演算部 303（に含まれる演算回路 312）は、ステップ S2706 の演算結果をハッシュ関数演算する。ここで、演算回路 312 は、第 7 の実施例のステップ S2305 と同様の演算処理を行う。

【0250】

ステップ S2708 において、制御/演算部 303（に含まれる演算回路 312）は、ステップ S2707 の演算結果と、選択された JPEG データとセットで入力されたデジタル署名データとを比較する。比較の結果、これらのデータが一致した場合には、JPEG データを正当なものと判断し、一致しなかった場合には、JPEG データに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【0251】

ステップS2709において、表示部304は、ステップS2708の比較結果、即ち不正な処理の有無を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したJPEGデータの正当性を視覚的に分かり易く認識することができる。

【0252】

尚、図27に示す一連の処理手順を制御するプログラムは、ROM305に格納されている。このプログラムは、制御／演算部303（に含まれる制御回路312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0253】

以上の手順により、選択されたJPEGデータの正当性を確認した場合、ユーザは、操作部306を操作し、該JPEGデータのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路310は各処理回路を制御し、該JPEGデータを廃棄することもできる。

【0254】

以上説明したように、第11の実施例では、第5の実施例の画像入力装置10にて撮像され、高能率符号化されたデジタル画像データの正当性を簡単な構成で、高速に確認することができる。又、上述のデジタル署名データを用いて、ある画像データがどの外部機器或いはどのユーザにて撮像されたかを特定することもできる。

【0255】

（第12の実施例）

第12の実施例では、画像検証装置20が、第6の実施例に基づいて生成されたデジタル署名データを用いて、JPEGデータの正当性を確認する構成について説明する。

【0256】

以下、図27を用いて第11の実施例の処理手順の一例について説明する。

【0257】

ステップS2701～S2704の処理は、上述の第11の実施例と同様の処

理としてその説明を省略する。

【0258】

ステップS2705において、制御／演算部303は、画像入力装置10の持つ固有の秘密情報をメモリ313から読み出し、外部装置40の持つ固有の秘密情報を外部I/F部301を介して入力する。そして、第6の実施例と同様に、これらの秘密情報を結合させ、新しい秘密情報を生成する。

【0259】

ステップS2706において、制御／演算部303（に含まれる演算回路312）は、上述の秘密情報とJPEGデータとを用いて、予め定められた規則に基づく所定の演算処理を行う。ここで、演算回路312は、第7の実施例のステップS2304と同様の演算処理を行う。

【0260】

ステップS2707において、制御／演算部303（に含まれる演算回路312）は、ステップS2706の演算結果をハッシュ関数演算する。ここで、演算回路312は、第7の実施例のステップS2305と同様の演算処理を行う。

【0261】

ステップS2708において、制御／演算部303（に含まれる演算回路312）は、ステップS2707の演算結果と、選択されたJPEGデータとセットで入力されたデジタル署名データとを比較する。比較の結果、これらのデータが一致した場合には、JPEGデータを正当なものと判断し、一致しなかった場合には、JPEGデータに何らかの不正な処理（即ち、改竄、偽造、合成等）が行われたと判断する。

【0262】

ステップS2709において、表示部304は、ステップS2708の比較結果、即ち不正な処理の有無を示す警告画像或いは警告メッセージを表示する。これにより、ユーザは、選択したJPEGデータの正当性を視覚的に分かり易く認識することができる。

【0263】

尚、図27に示す一連の処理手順を制御するプログラムは、ROM305に格

納されている。このプログラムは、制御／演算部 303（に含まれる制御回路 312）によって読み出され、所望の画像の検証を指示する毎に起動する。

【0264】

以上の手順により、選択された J P E G データの正当性を確認した場合、ユーザは、操作部 306 を操作し、該 J P E G データのデコード、表示、加工及び編集を指示することができる。又、正当性が確認されなかった場合、制御回路 310 は各処理回路を制御し、該 J P E G データを廃棄することもできる。

【0265】

以上説明したように、第 12 の実施例では、第 6 の実施例の画像入力装置 10 にて撮像され、高能率符号化されたデジタル画像データの正当性を簡単な構成で、高速に確認することができる。又、上述のデジタル署名データを用いて、ある画像データがどの外部機器と接続された画像入力装置或いはどのユーザによって使用された画像入力装置にて撮像されたかを特定することもできる。

【0266】

尚、本発明はその精神、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

【0267】

例えば、第 1 ～ 第 6 の実施例では、画像入力装置 10 内においてデジタル署名データを生成したが、該デジタル署名データを画像入力装置 10 に接続された外部装置 40 にて生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、高能率符号化されたデジタル画像データ等を画像入力装置 10 から外部装置 40 に送信し、生成処理を開始する。

【0268】

又、第 1 ～ 第 6 の実施例では、デジタル署名データの生成に必要な演算処理を画像入力装置 10 と外部装置 40 とに分散させ、各装置が共同してデジタル署名データを生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、高能率符号化されたデジタル画像データ等の中で必要な部分のみを画像入力装

置 1 0 から外部装置 4 0 に送信し、生成処理を開始する。

【0 2 6 9】

又、第 7 ～第 1 2 の実施例では、画像検証装置 2 0 が外部入力されたデジタル画像データを用いてデジタル署名データを生成したが、該デジタル署名データを画像検証装置 2 0 に接続された外部装置 4 0 にて生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、外部入力されたデジタル画像データ等を画像検証装置 2 0 から外部装置 4 0 に送信し、生成処理を開始する。

【0 2 7 0】

又、第 7 ～第 1 2 の実施例では、デジタル署名データの生成に必要な演算処理を画像検証装置 2 0 と外部装置 4 0 とに分散させ、各装置が共同してデジタル署名データを生成することも可能である。このように構成した場合、各装置が互いの装置を認証した後、デジタル署名データの生成に必要な処理プログラム、外部入力されたデジタル画像データ等の中で必要な部分のみを画像検証装置 2 0 から外部装置 4 0 に送信し、生成処理を開始する。

【0 2 7 1】

又、第 7 ～第 1 2 の実施例では、図 2 4 ～図 2 7 に示す一連の処理手順を制御するプログラムは、所望の画像の検証を指示する毎に起動する構成として説明したが、所望の画像を外部入力することに自動的に起動するように構成してもよい。

【0 2 7 2】

従って、前述の実施例はあらゆる点において単なる例示に過ぎず、限定的に解釈してはならない。

【0 2 7 3】

【発明の効果】

以上のように、本発明によれば、デジタルデータの著作権を保護すると共に、そのデジタルデータに対する不正な処理（改竄、偽造、合成等）を検出するための署名データを簡単な構成で、高速に生成することができる。又、その署名データを用いて、デジタルデータに対する不正な処理（改竄、偽造、合成等）

を簡単な構成で、高速且つ確実に検出することができる。

【0274】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの機器によって生成されたかを特定することができる。

【0275】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの機器によって生成されたかを特定することができる。

【0276】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器に接続された外部機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの外部機器と接続された機器或いはどのユーザによって使用された機器にて生成されたかを特定することもできる。

【0277】

又、本発明によれば、デジタルデータとそのデジタルデータを生成した機器の秘密情報とその機器に接続された外部機器の秘密情報とを用いて署名データを生成することにより、あるデジタルデータがどの外部機器と接続された機器或いはどのユーザによって使用された機器にて生成されたかを特定することもできる。

【図面の簡単な説明】

【図1】

本実施例のデジタル画像検証システムについて説明する図。

【図2】

本実施例の画像入力装置10の基本構成について説明するブロック図。

【図3】

本実施例の画像検証装置20の基本構成について説明するブロック図。

【図4】

第1の実施例の処理手順を説明するフローチャート。

【図 5】

第 1 の実施例における所定の演算処理を説明する図。

【図 6】

第 2 の実施例の処理手順を説明するフローチャート。

【図 7】

第 2 の実施例における J P E G データを表す図。

【図 8】

第 2 の実施例における秘密情報を説明する図。

【図 9】

第 2 の実施例における所定の演算処理を説明する図。

【図 1 0】

第 2 の実施例におけるハッシュ関数演算の第 1 のモードを説明する図。

【図 1 1】

第 2 の実施例におけるハッシュ関数演算の第 2 のモードを説明する図。

【図 1 2】

第 2 の実施例におけるハッシュ関数演算の第 3 のモードを説明する図。

【図 1 3】

第 1 ～第 3 のモードにおける使用される初期値を説明する図。

【図 1 4】

第 3 の実施例の処理手順を説明するフローチャート。

【図 1 5】

第 3 の実施例における秘密情報を説明する図。

【図 1 6】

第 3 の実施例における C B C モードを説明する図。

【図 1 7】

第 3 の実施例における C F B モードを説明する図。

【図 1 8】

第 3 の実施例における O F B モードを説明する図。

【図 1 9】

第 4 の実施例の処理手順を説明するフローチャート。

【図 2 0】

第 4 の実施例における秘密情報を説明する図。

【図 2 1】

第 5、第 6 の実施例の処理手順を説明するフローチャート。

【図 2 2】

画像入力装置 1 0 と外部装置 4 0 との相互認証処理を説明する図。

【図 2 3】

第 7 の実施例の処理手順を説明するフローチャート。

【図 2 4】

第 8 の実施例の処理手順を説明するフローチャート。

【図 2 5】

第 9 の実施例の処理手順を説明するフローチャート。

【図 2 6】

第 1 0 の実施例の処理手順を説明するフローチャート。

【図 2 7】

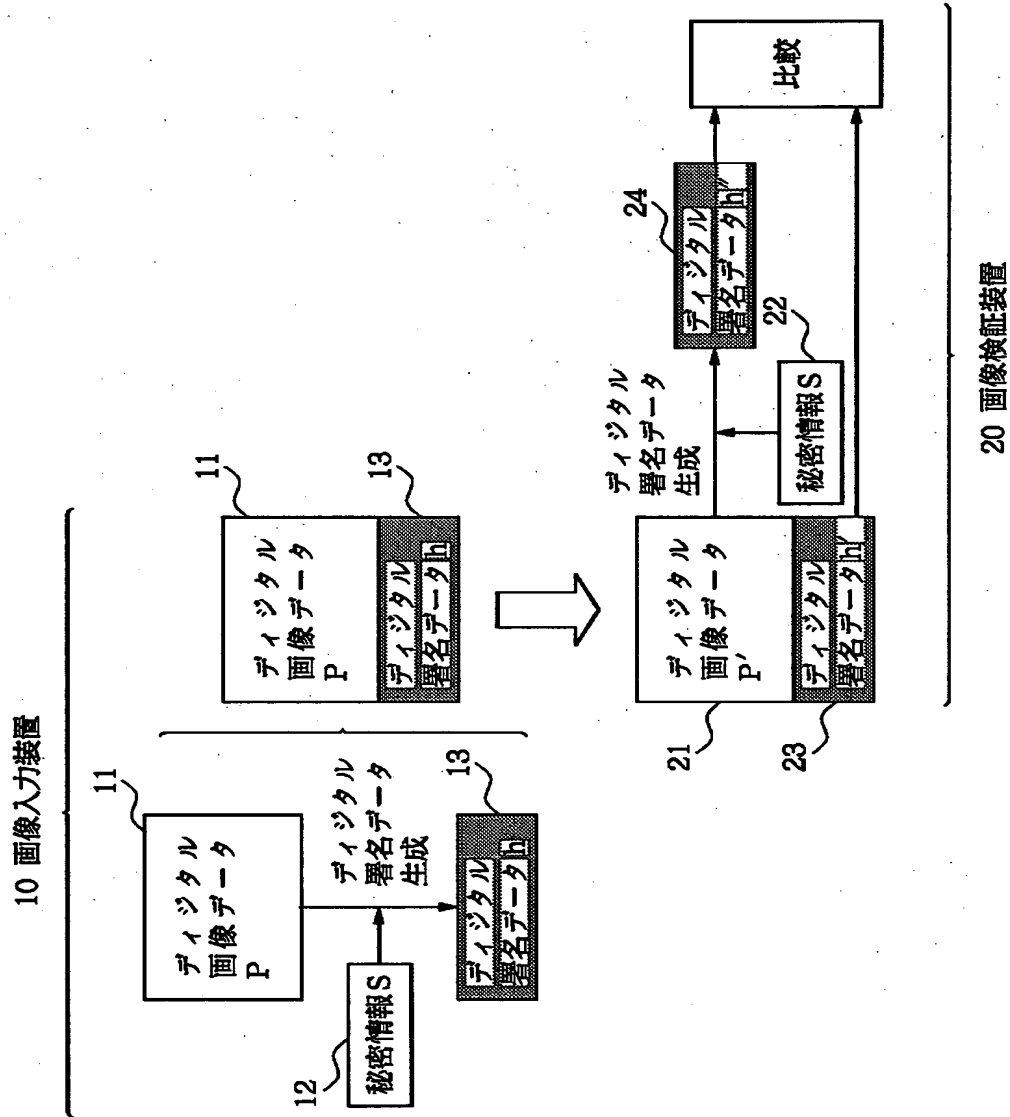
第 1 2 の実施例の処理手順を説明するフローチャート。

【図 2 8】

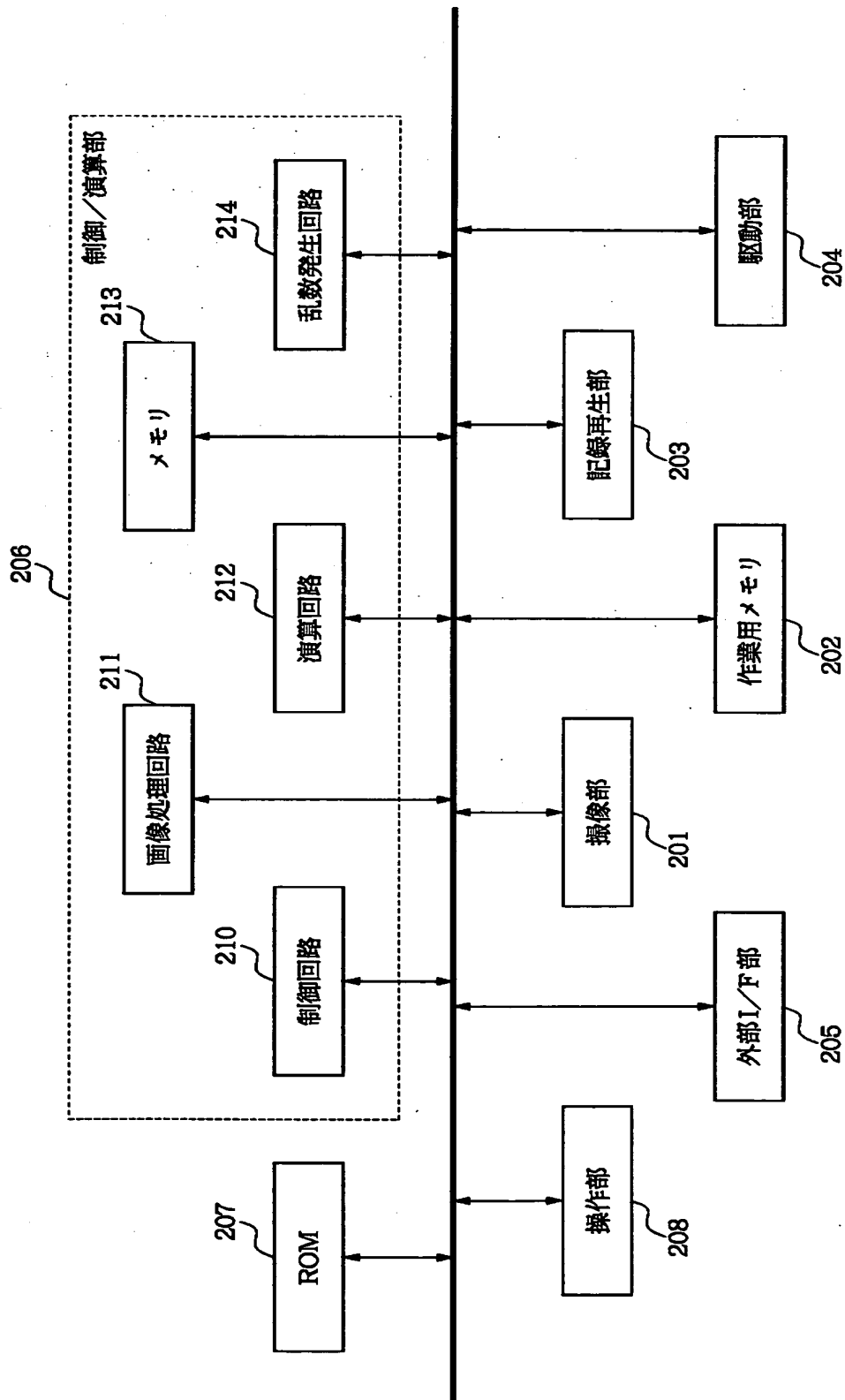
従来のシステムを説明する図。

【書類名】 図面

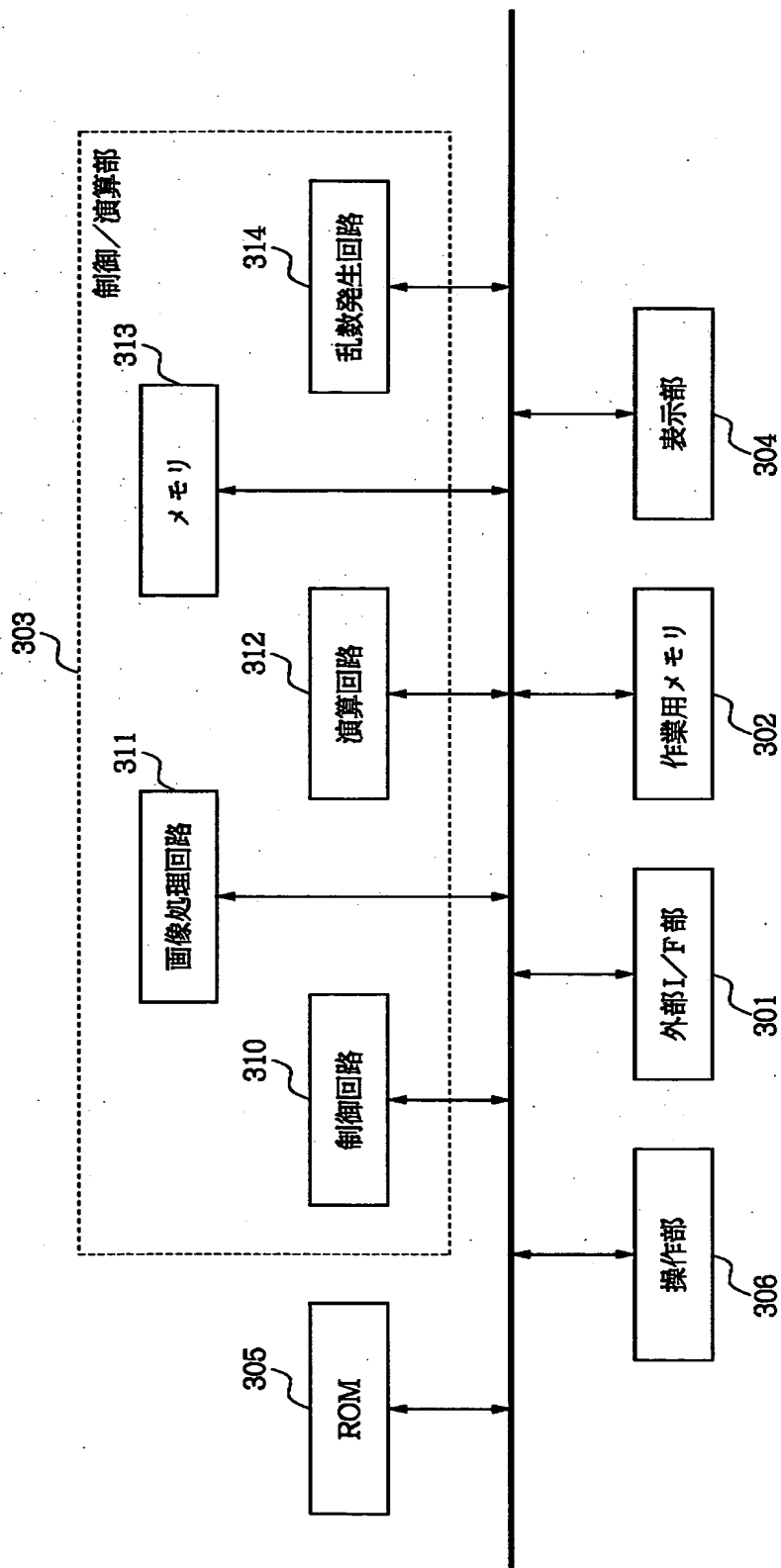
【図 1】



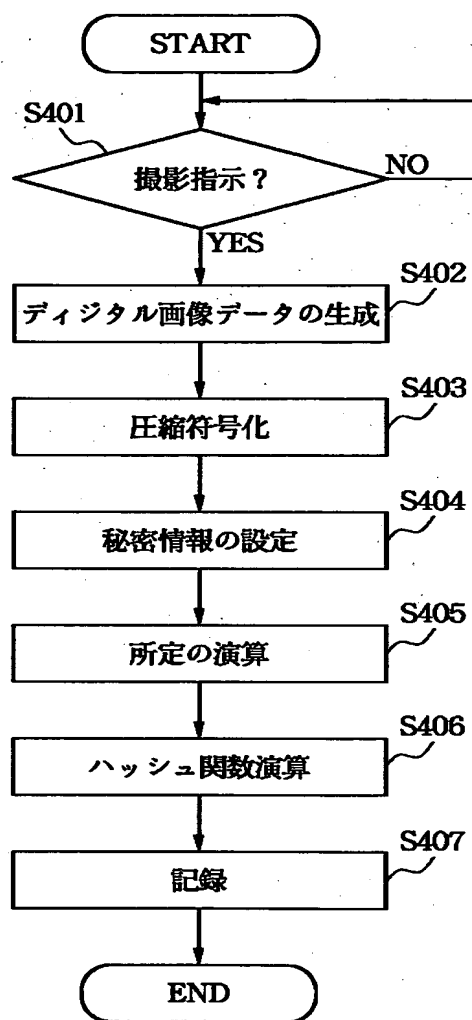
【図 2】



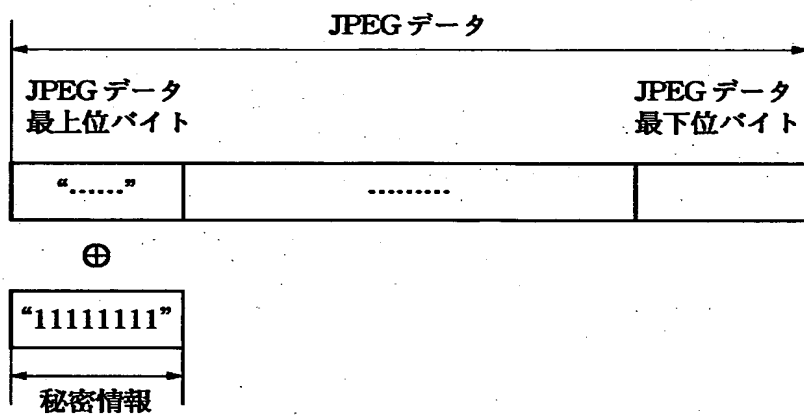
【図 3】



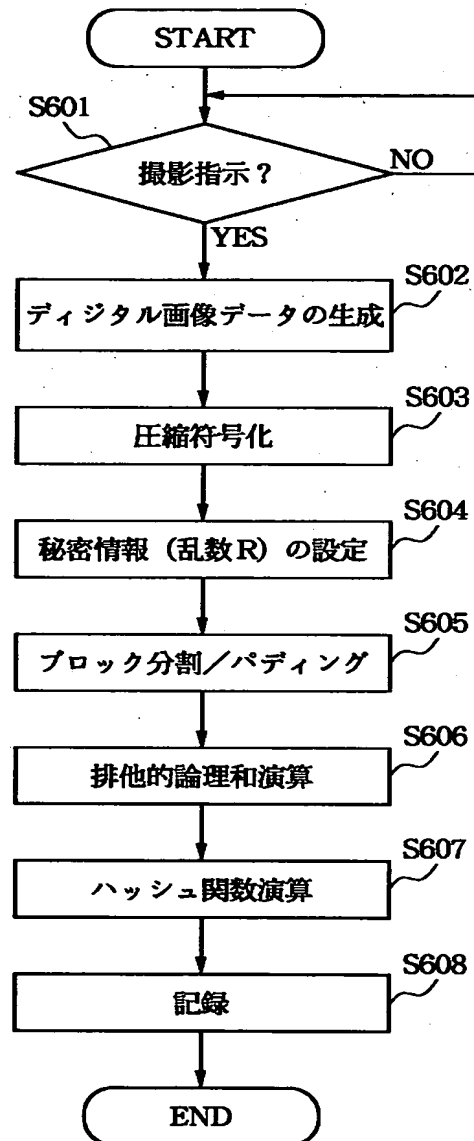
【図 4】



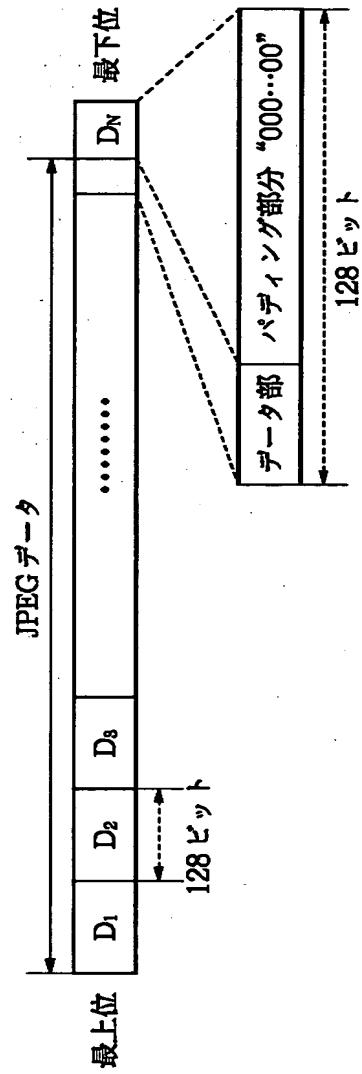
【図 5】



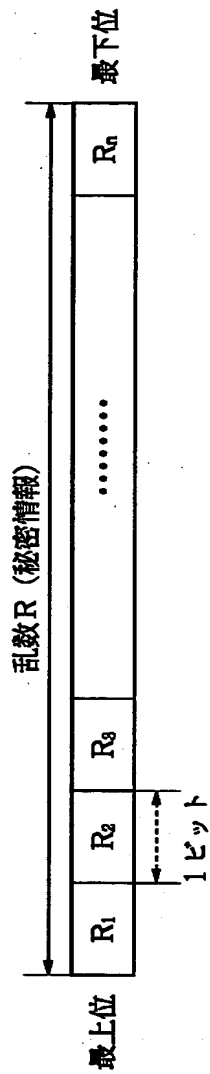
【図 6】



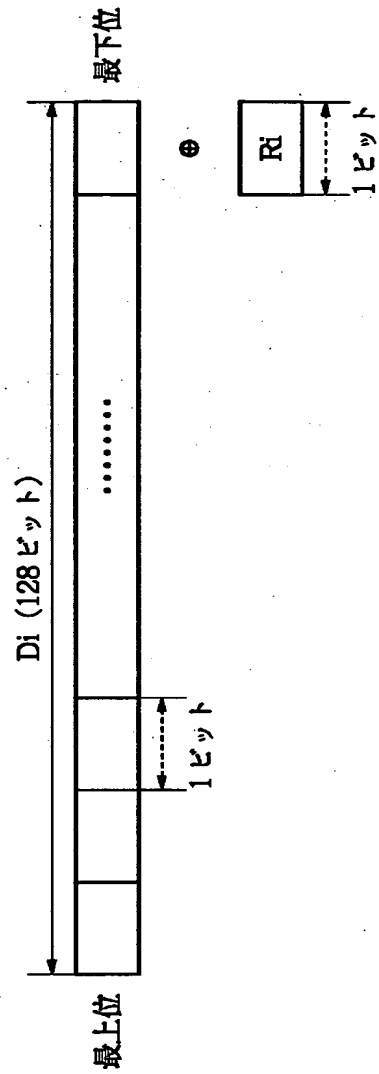
【図 7】



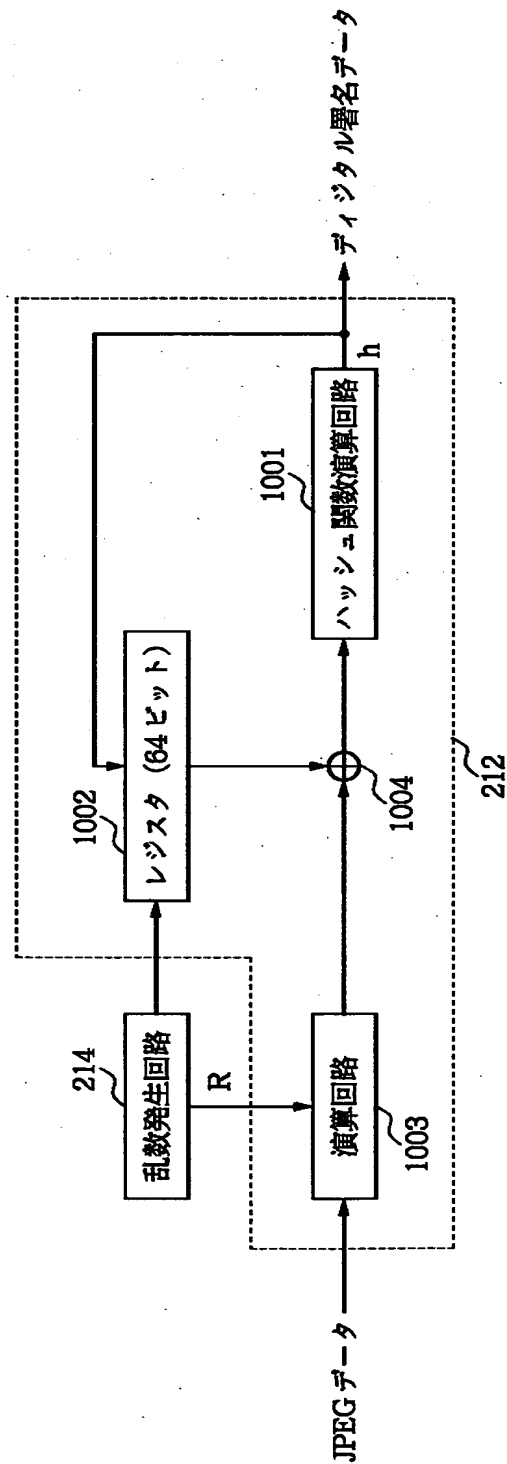
【図 8】



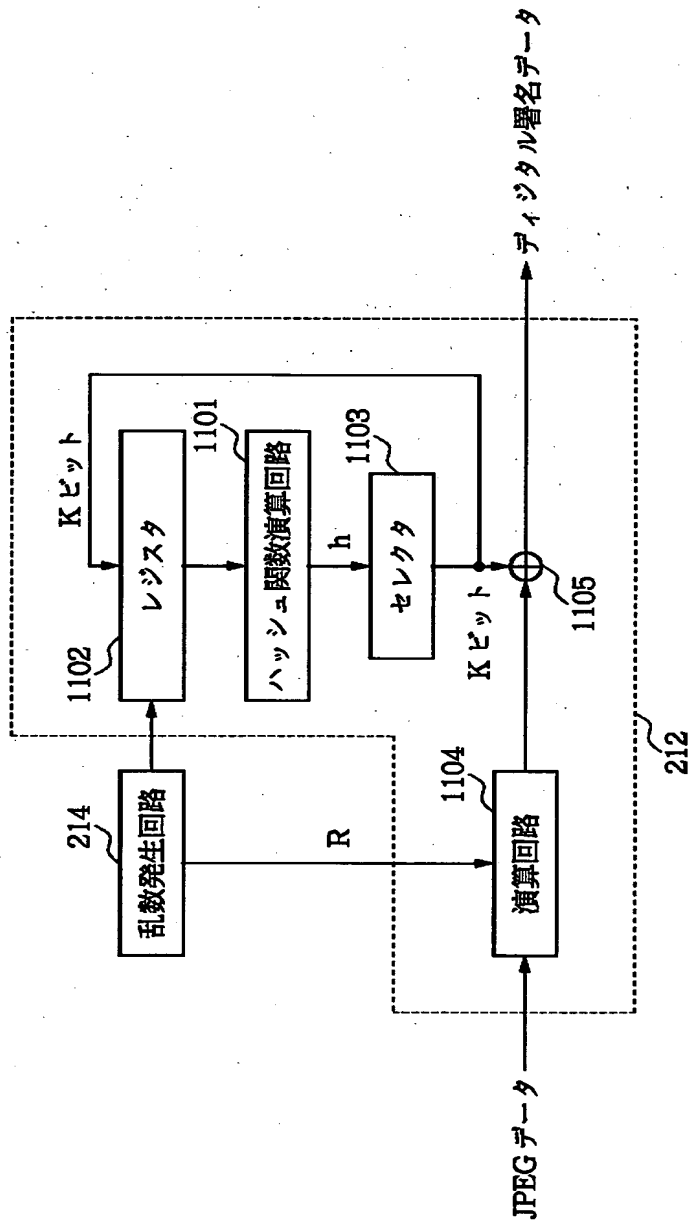
【図 9】



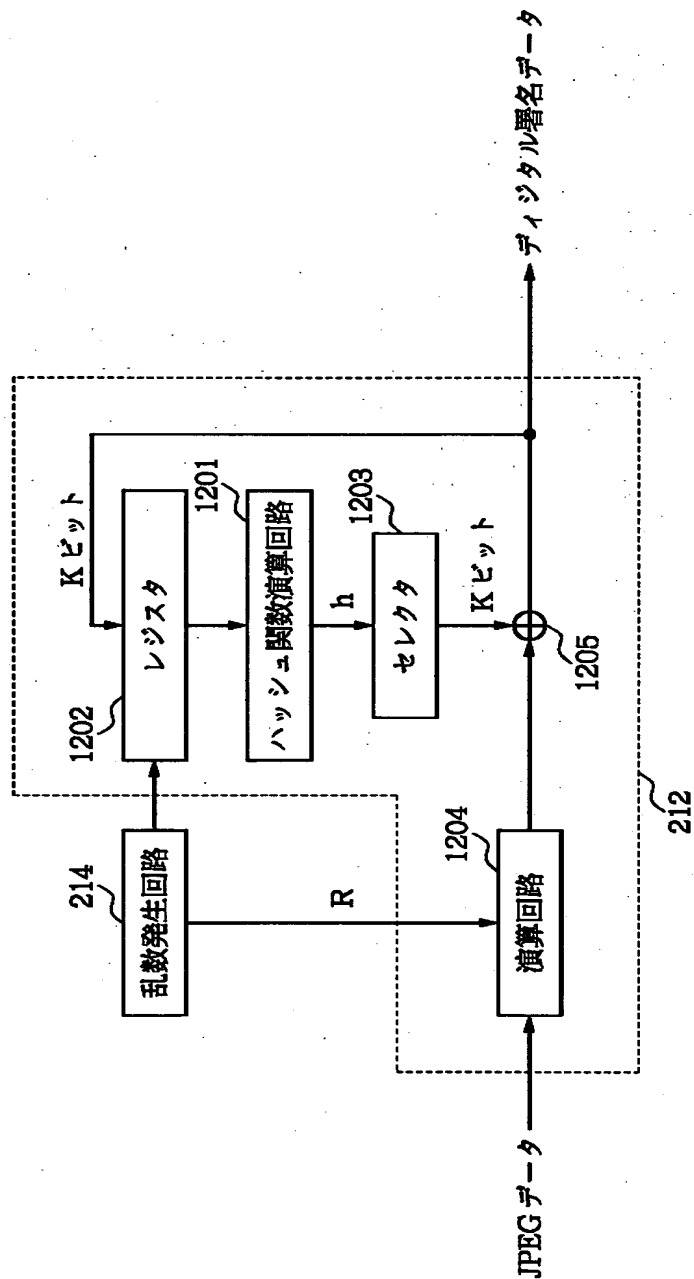
【図 1 0】



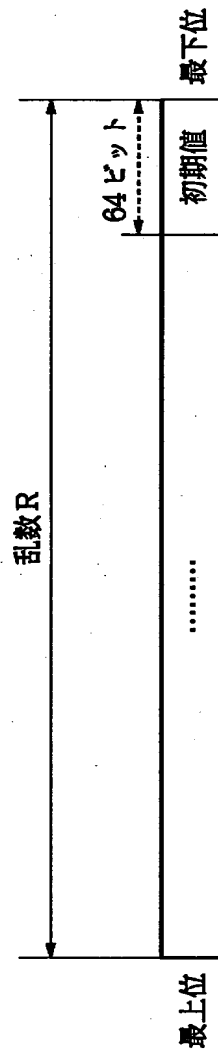
【図 11】



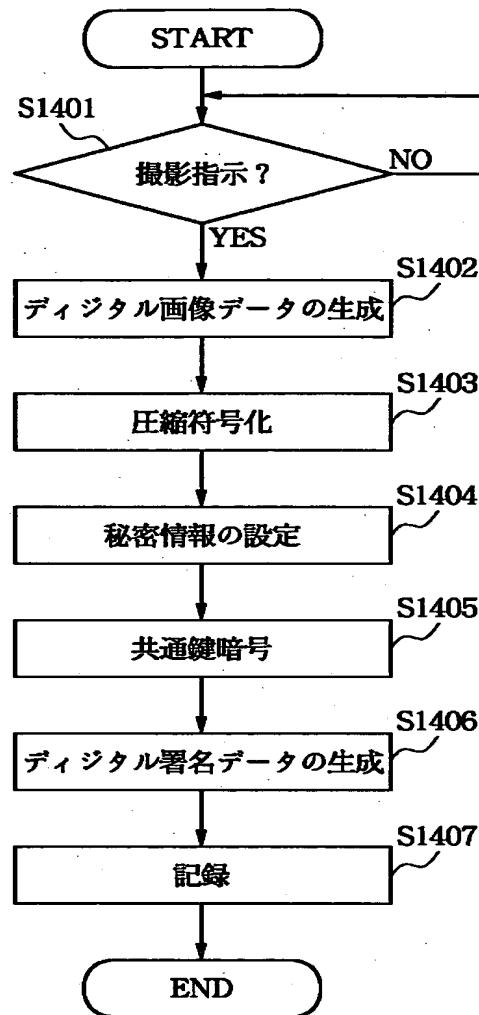
【図 1 2】



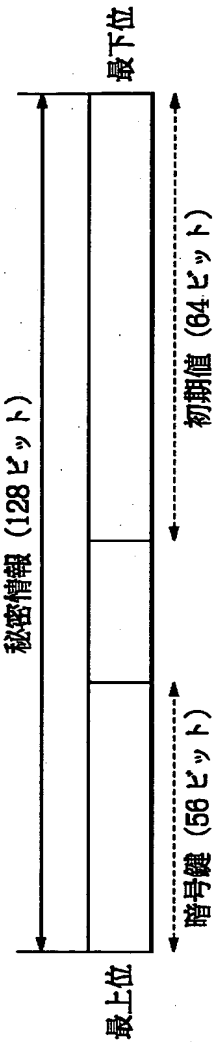
【図 1 3】



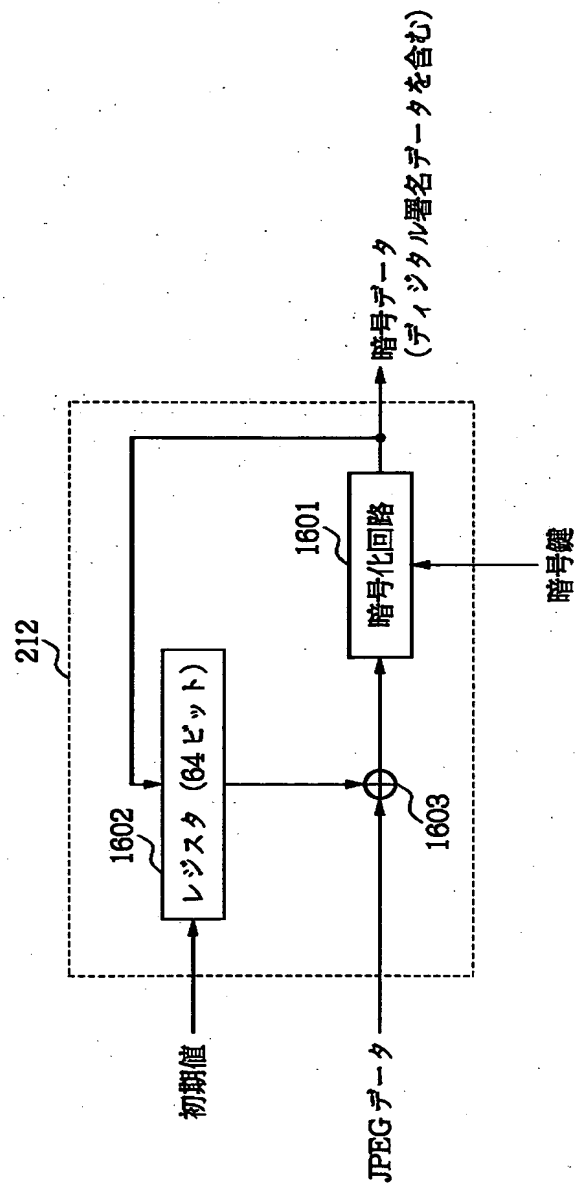
【図 14】



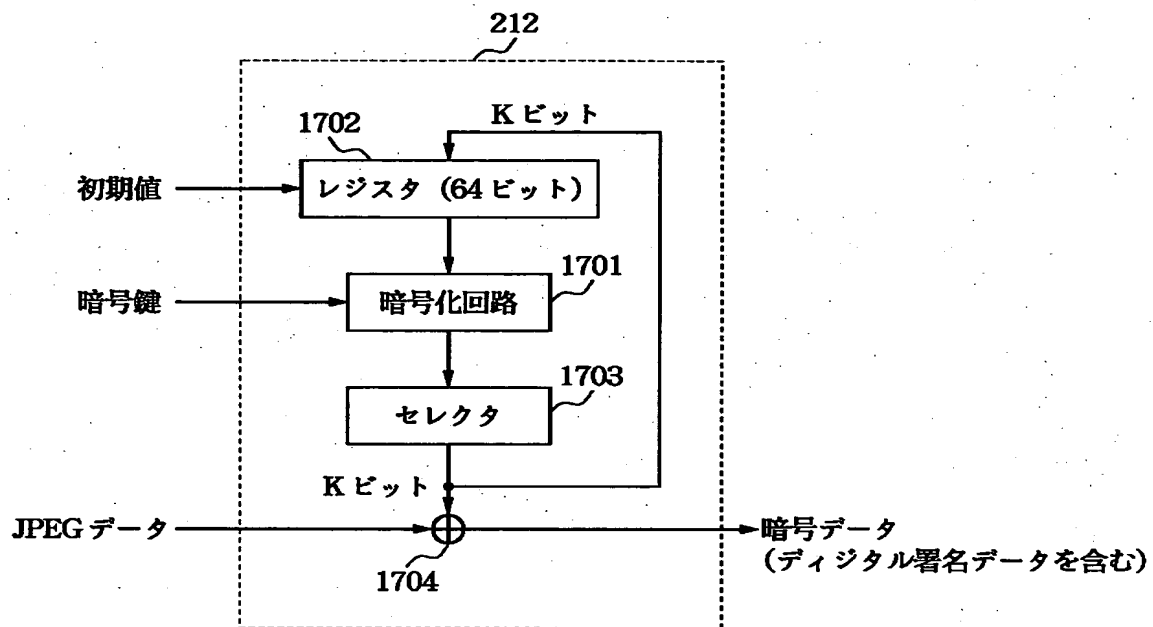
【図 1 5】



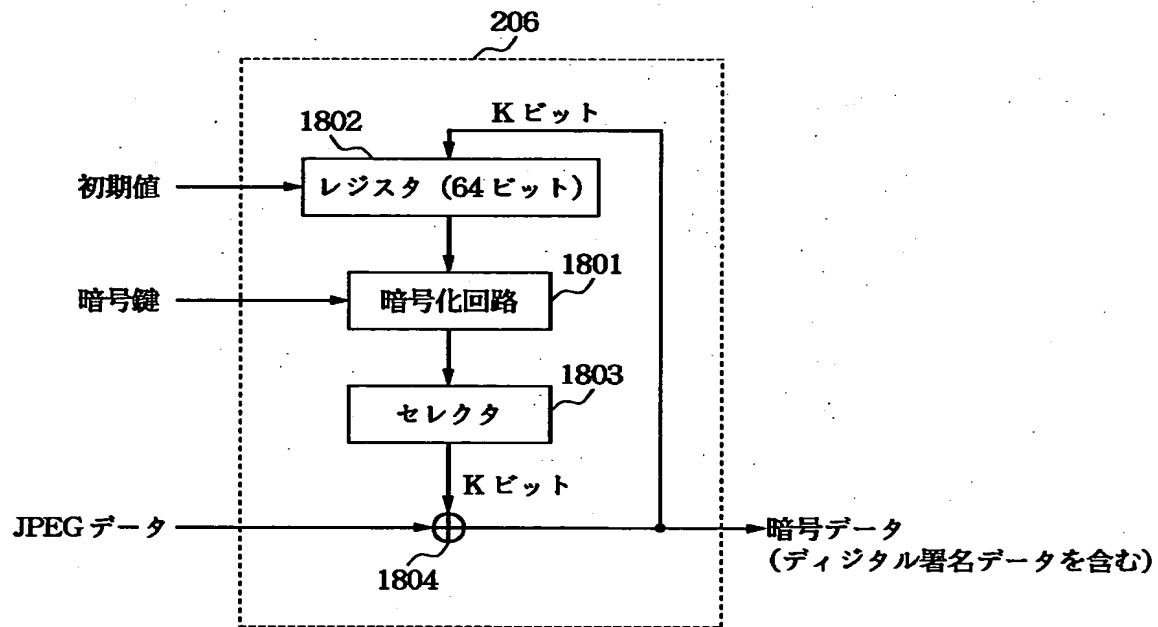
【図 1 6】



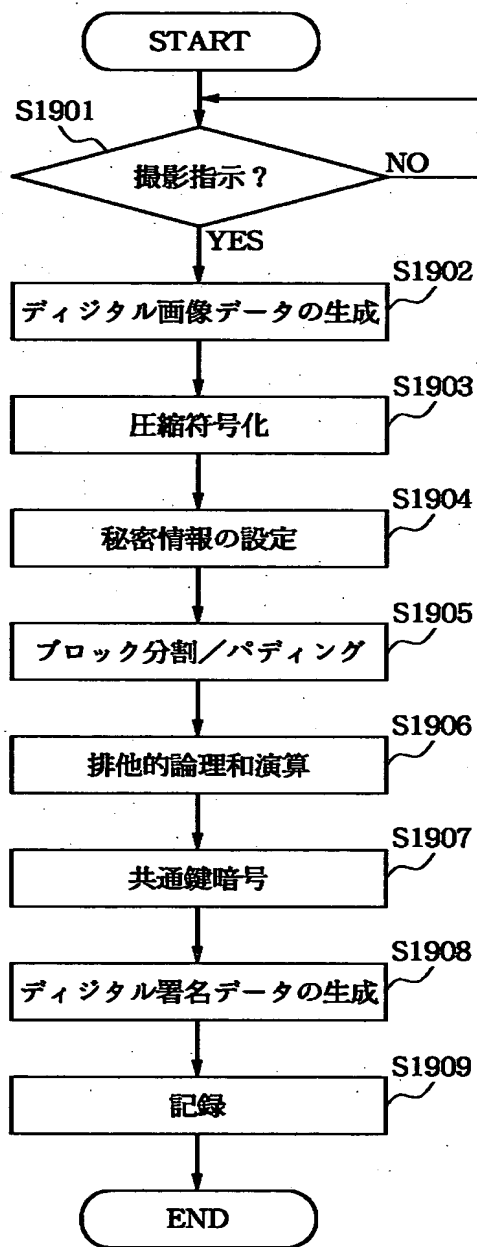
【図 1 7】



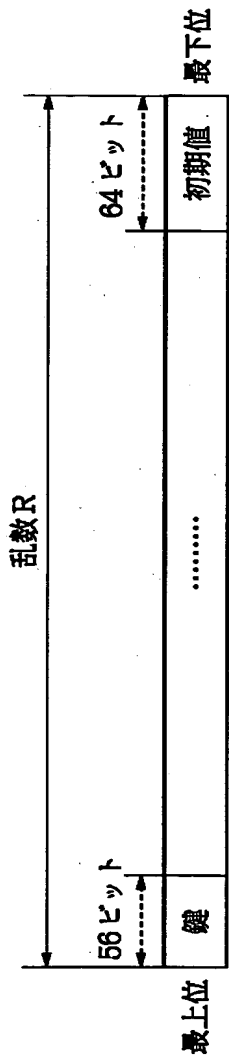
【図 18】



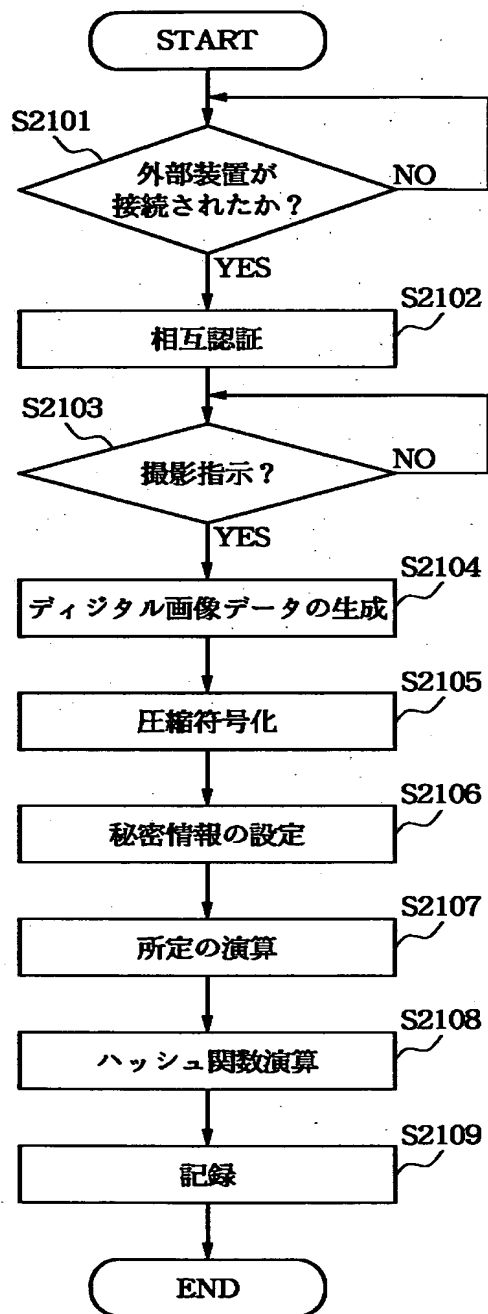
【図 19】



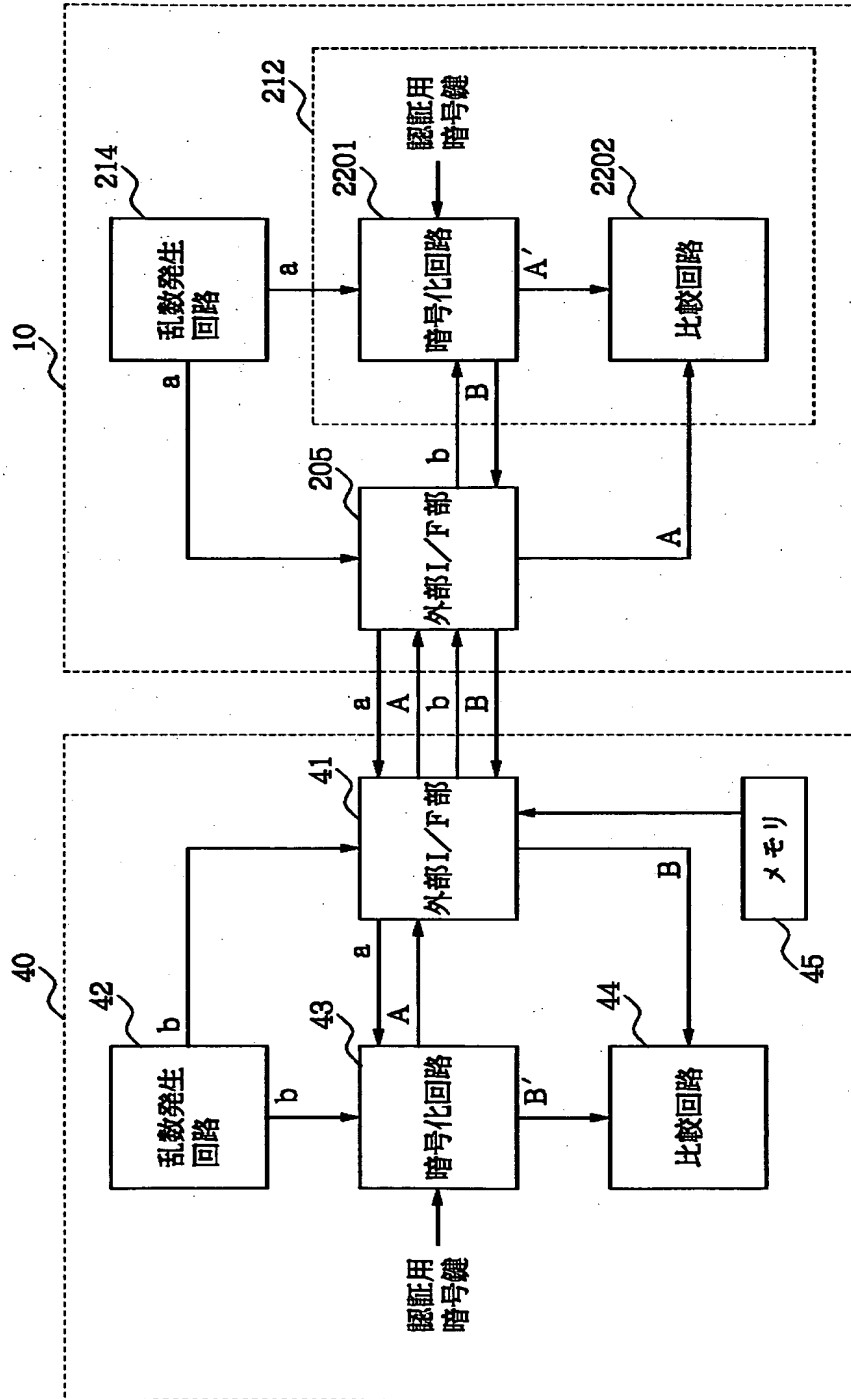
【図 2 0】



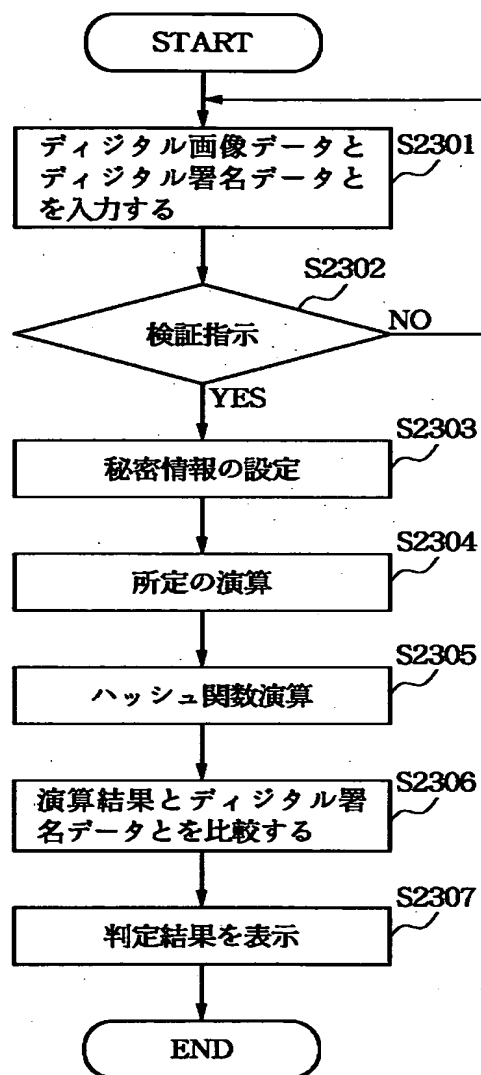
【図 21】



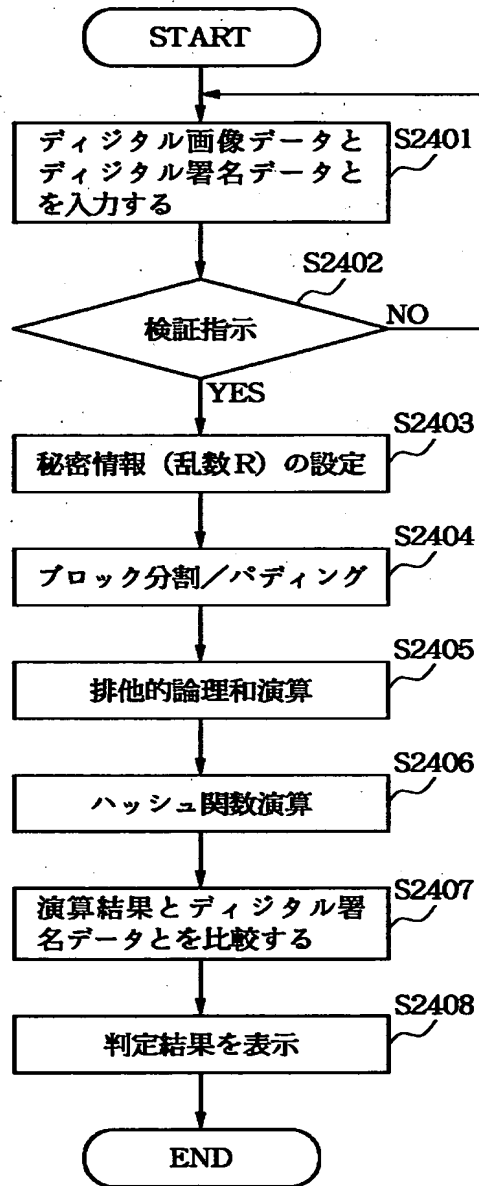
【図 2 2】



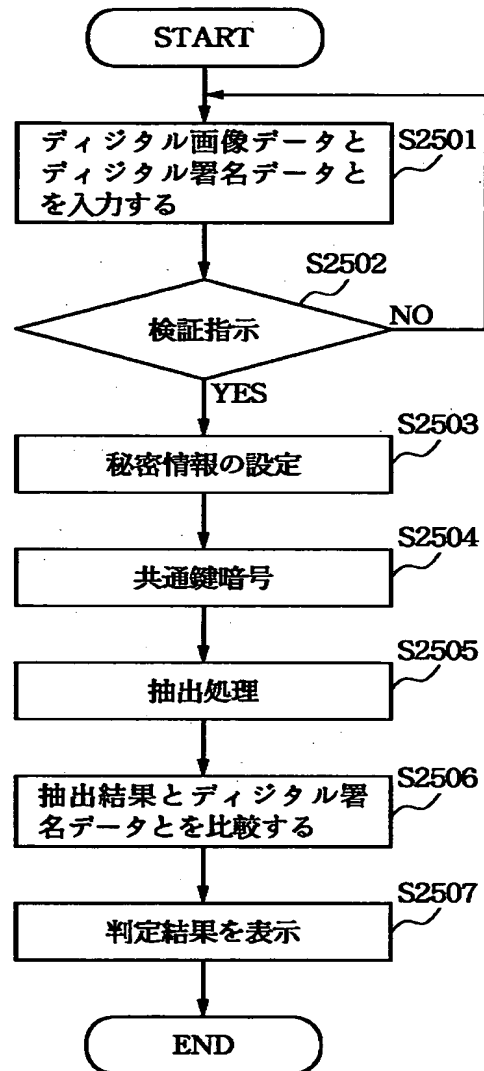
【図 2 3】



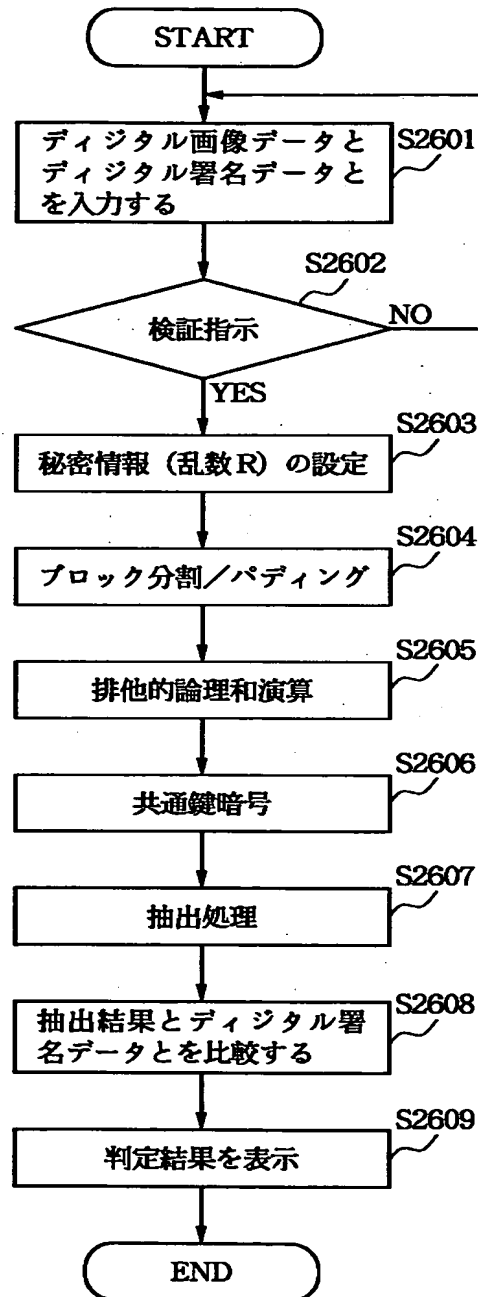
【図 2 4】



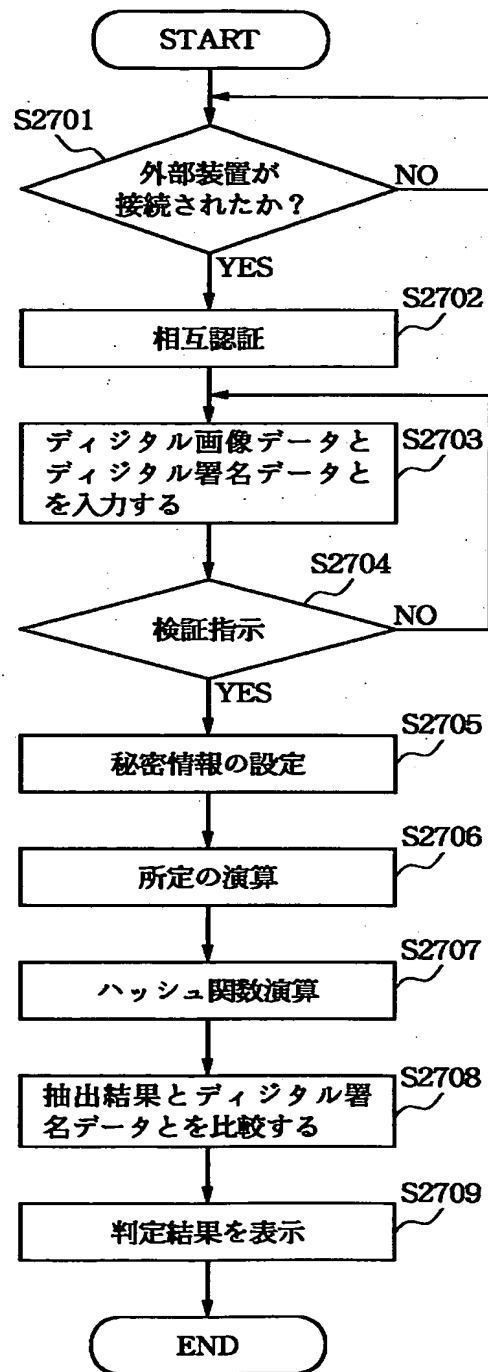
【図 2 5】



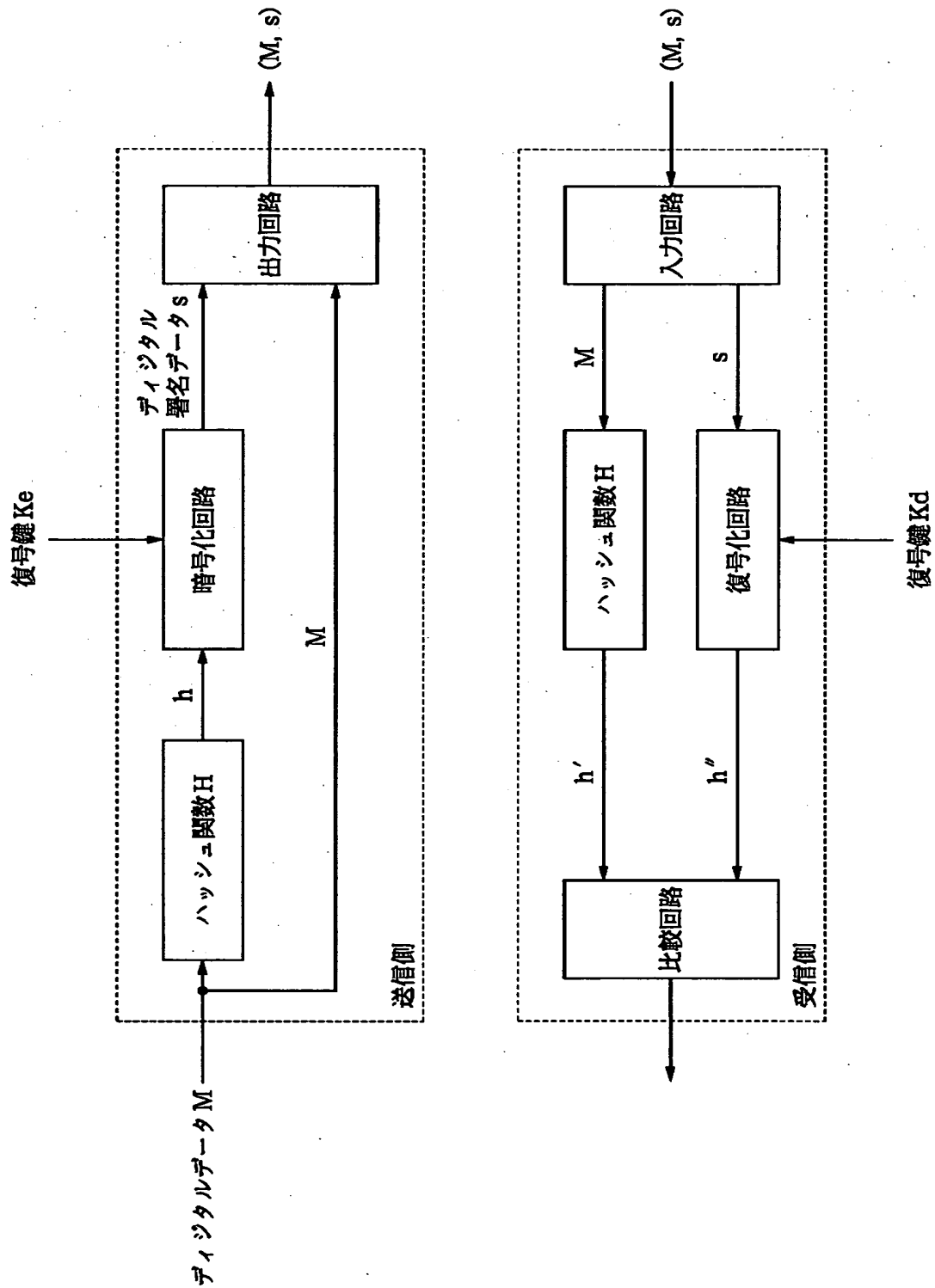
【図 26】



【図 27】



【図 28】



【書類名】 要約書

【要約】

【課題】 デジタルデータの正当性を検証することのできる技術を提供する。

【解決手段】 第1の画像処理装置10は、デジタル画像11と秘密情報12とを用いて所定の演算を行い、その演算結果を用いて該デジタル画像に対する不正な処理を検出するため署名データ13を生成する。第2の画像処理装置20は、そのデジタル画像11と秘密情報22とを用いて所定の演算を行い、その演算結果と上述の署名データ13とを比較してそのデジタル画像11に対する不正な処理の有無を検出する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都大田区下丸子3丁目30番2号
氏 名 キヤノン株式会社